US Signal - OneNeck IT Solutions Legacy Service Catalog

Family: Advanced Services

Category: Engineering

100500 Network Engineer Resource

Company's Responsibilities and Included Features

- Provide a Networking Engineer skill-set resource based upon the hours per month specified on the Executed Order.
- The service hour quantity specified on the Executed Order must be used before the end of each calendar month. Unused hours will be foreit if not consumed. Unused hours do not roll over to the next month.
- Company Services will be performed during standard business hours of 8:00am to 5:00pm (local time), Monday through Friday excluding holidays recognized by Company.
- Expenses, excluding local travel (mileage), will be billed as incurred.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client assumes the following responsibilities required to complete the services provided herein (Services). Company may charge for actual additional work and expense incurred if Client fails to perform these responsibilities according to a mutually agreed schedule.

- Assign Point-Of-Contact. Assign a single Client representative to facilitate communications, assemble Client resources, coordinate Client activities, accept deliverables, and perform any change orders.
- Coordinate Client Activities. Coordinate all Client activities and 3rd party activities, other than activities of Company and Company subcontractors, required for this project. Client is responsible for the timely performance of activities of their staff and other contractors according to the agreed project schedule, unless subcontracted through Company.
- Separate Provisioning. Client must separately provide or purchase all equipment, cabling, circuits, 3rd party services, software, licenses, manufacturer maintenance and support for the solution. Any exceptions are explicitly identified in the Pricing section below.
- Ensure Compliance. Client will ensure compliance with any national or local safety and building regulations or similar requirements affecting installation.
- Facilities Readiness. Client will ensure facilities are ready for equipment installation as scheduled, including mounting location, power, cooling, premise cabling, and patch cables not supplied by Company. Facilities must meet equipment installation requirements as provided herein and by any applicable manufacturer documentation.
- Access to Facilities. Client will provide access to their facilities as required to perform this SOW as scheduled.
- Access to Equipment. Client will provide physical access, passwords, access codes or security devices as necessary to perform the Services.
- Remote Access to Equipment. Client will provide Company staff VPN (virtual private network) remote access to the Client equipment required to perform the Services.

- Timely Performance. Client will work with Company in a timely fashion to complete project tasks, testing, and acceptance of deliverables according to mutually agreed schedules.
- Services Scheduling. A mutually agreed schedule for Company Services shall be developed.

610417 Network Service Engineer

Company's Responsibilities and Included Features

Network Engineer

- Provide a fully dedicated Service Delivery Executive to the Client.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Receive the service.

Family: Cloud and Hosting Solutions

Category: Backup

600268 Backup Storage

Company's Responsibilities and Included Features

-Present shared SAN space to hosted environment leveraging Company's shared SAN infrastructure
-Administration of the SAN Storage Systems includes:
-Backend disk storage management including:
-RAID group configuration
-Volume configuration
-SAN: LUN provisioning
-Monitoring and reporting of disk space usage
-Triage and troubleshoot SAN/NAS infrastructure, performance and presentation issues
-Global settings/configuration management including LUN definitions
-SAN: Dynamic/Redundant path presentation. (may require proprietary multi-path software) (if applicable)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Backup environment compute, network Infrastructure and software.

600308 CommVault Licensing

Company's Responsibilities and Included Features

Licensing

- Company will provide CommVault backup software licensing for the purpose of operating an on-premise, Client provided infrastructure, solution for backup.
- Licensing is for an unlimited number of data agents
- Licensing is inclusive of the following data types:
  - Hypervisor-based data protection
  - Filesystem based data protection
  - Application-based data protection

- Licensing excludes the following features
  - CommVault Live Sync replication
  - CommVault IntelliSnap

Service Fees

The service is charged upon the total amount of front end protected gigabytes (GB) from the system. Front-end protected gigabytes are defined as the amount of application data protected as read from the source application (server). The service fee is assessed monthly and per whole GB.

Metering

The service fee is assessed monthly. The size of the protected data is measured by the size of the largest full, uncompressed, un-deduplicated backup, during the billing period, as measured by the backup system. The unit of measurement is protected GB.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Infrastructure

- Client must provide the necessary hardware (network, servers, storage) to run the backup software
- Definition of what needs to be backed up
- Define the window of time within which the weekly full backup may be initiated
- Operating system administration of servers being backed up
- Installation and management of backup agents on servers being backed up if local agents are required
- Validation of data restored

Required Services

- Client must subscribe to Company's managed services for on-premise backup system server roles.

600360 Database Log Backups option - 15 minute (requires Standard or Premium backup on DB server)

Company's Responsibilities and Included Features

- Requires Standard or Premium backup services on DB server
- Incremental backups configured to run every 15 minutes
- Full backups configured to run weekly during client specified backup window
- Restoration start time objective: 1 hour
- Retention: 8 days (Maximum time window to choose a restoration point)
- Backups processed from the client hosted environment to company backup storage infrastructure
- Backup job monitoring, reporting and notification
- Advanced administration support for backup infrastructure issues including triage of backup failures
- Support for initiating backup restorations (standard support SLA based on ticket severity)
- Company provided engineering support for agent software upgrades as dictated by server side application software
- Initial configuration of agent software and backend infrastructure components
- All subsequent adds/moves and changes to the agent and backend backup infrastructure including inclusions and exclusions from backup
- Incident ticket creation and tracking
- Service availability announcements (e.g. scheduled and unscheduled maintenance)

- Operate the service infrastructure and provide an escalation point for technical support related requests
- Management and execution of regular service operations
- Support and troubleshooting for client side technical issues
- Service capacity management
- Implementation of major changes to the service
- Ad-Hoc technical requests
- Provide support to service desk and service administrator personnel and act as an escalation point
- Last line of support before escalating to vendor support for product issues.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Responsible for the consumption of this service
- Escalation point on the Client side

600602 ReliaCloud Backup Client License for Hypervisor Backup

Company's Responsibilities and Included Features

ReliaCloud Backup Client License for Hypervisor Backup is a Company-provided backup software agent that leverages the hypervisor of the virtual server to protect a specific type of data, in this case the entire virtual machine.

This service requires the use of a ReliaCloud storage service, local pod, remote pod, or an on-premises appliance (separate Item IDs).

This service is delivered as a metered service allowing Client to consume software licensing in a pay-as-you-go monthly model.

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup, and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General operating system level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This is a metered service.
- The number of clients is determined by the number of unique clients of this type (VM based) which are active for at least one (1) period within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is per server.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Backup Operation

- Define backup content
- Define frequency, schedule, location, and retention of the backups
- Conduct operating system administration of servers subject to backup
- Validate data restored
- Install and manage backup agents on servers subject to backup if local agents are required
- Install any associated software (agents) on servers or infrastructure to be backed up

600603 ReliaCloud Backup Client License for Hypervisor / File System Backup

Company's Responsibilities and Included Features

ReliaCloud Backup Client License for Hypervisor / File System Backup is a Company-provided backup software agent that allows for physical server backup and data protection down to the file level. It also can be used in conjunction with hypervisor-based backups for virtual servers to protect data to the file level.

This service requires the use of a ReliaCloud storage service, local pod, remote pod, or an on-premises appliance (separate Item IDs).

This service is delivered as a metered service allowing Client) to consume software licensing in a pay-as-you-go monthly model.

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup, and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General operating system level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This is a metered service.
- The number of clients is determined by the number of unique clients of this type (file system) that is active for at least one (1) period within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is per server.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Backup Operation

- Define backup content
- Define frequency, schedule, location, and retention of the backups
- Conduct operating system administration of servers subject to backup
- Validate data restored
- Install and manage backup agents on servers subject to backup if local agents are required
- Install any associated software (agents) on servers or infrastructure to be backed up

600604 ReliaCloud Backup Client License for Hypervisor / File System / Application Backup

Company's Responsibilities and Included Features

ReliaCloud Backup Client License for Hypervisor / File System / Application Backup is a Company-provided backup software agent that allows for application-based data protection. It also can be used in conjunction with hypervisor-based backups for virtual servers, physical server backups, and to protect data to the file level.

This service requires the use of a ReliaCloud storage service, local pod, remote pod, or an on-premises appliance (separate Item IDs).

This service is delivered as a metered service allowing Client (to consume software licensing in a pay-as-you-go monthly model.

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup, and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General operating system level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This is a metered service.

- The number of clients is determined by the number of unique clients of this type (application) that are active for at least one (1) period within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is per server.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Backup Operation

- Define backup content
- Define frequency, schedule, location, and retention of the backups
- Conduct operating system administration of servers subject to backup
- Validate data restored
- Install and manage backup agents on servers subject to backup if local agents are required
- Install any associated software (agents) on servers or infrastructure to be backed up

600605 ReliaCloud Backup Service for ReliaCloud - Local Pod Storage

Company's Responsibilities and Included Features

ReliaCloud Backup Service - Local Pod Storage provides the primary storage target for the purpose of facilitating backup storage within the primary ReliaCloud Pod (site) that the backup service is conducted from. This service requires a subscription to Company-provided backup client licensing services (separate Item IDs).

Service Metering

- This is a metered service.
- The size of the stored data is measured as the largest peak size in GB during the month stored within designated ReliaCloud Pod sites. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Service Level Agreement (SLA)

- SLA for service availability is 100%

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Subscribe to ReliaCloud Backup Client License service(s)

600606 ReliaCloud Backup Service for Colocation - Local Pod Storage

Company's Responsibilities and Included Features

ReliaCloud Backup Service for Colocation - Local Pod Storage provides the primary storage target for the purpose of facilitating backup storage within the primary Colocation facility that the backup service is conducted from. This service requires a subscription to Company-provided backup client licensing services (separate Item IDs).

Service Connectivity

This service is provided to the colocation environment to a single demarcation within Client's colocation infrastructure, and is delivered over a Cat6 ethernet cable as part of a Backup Area Network (BAN).

Service Metering

- This is a metered service.
- The size of the stored data is measured as the largest peak size in GB during the month stored within designated ReliaCloud Pod sites. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Service Level Agreement (SLA)

- SLA for the service availability is 99.99%

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Subscribe to ReliaCloud Backup Client License service(s)
- Provide a network port to terminate the Company's Cat6 ethernet connection
- Design and implement a network security policy between Client's network and Company's BAN

600608 ReliaCloud Backup Service for On-Prem. - 10 TB Appliance

Company's Responsibilities and Included Features

ReliaCloud Backup Service for On-Prem. 10 TB Appliance (Appliance) provides a local storage appliance for the purpose of facilitating backups with local storage capacity up to 10 terabytes (TB) of usable storage capacity. This service requires a subscription to Company-provided backup client licensing services.

A client refers to a software agent installed on the computer, physical or virtual server, or database to protect a specific type of data.

This service is delivered as a metered service allowing the Client to consume the storage in a pay-as-you-go model up to the maximum capacity of the Appliance (10 TB).

On-Premises Appliance

- Maintain ongoing support contracts for all hardware and software involved in the operation and support of the Appliance
- Manage service capacity
- Monitor Appliance health
- Repair or replace (as necessary) equipment
- Maximum appliance storage capacity of 10TB usable
- Two (2) 10 Gb network ports

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup, and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their solution
  - General operating system level troubleshooting
  - Escalation to the software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions

- Document user issues and system errors

Service Metering

- This is a metered service.
- The size of the stored data is measured as the largest peak size in GB during the month stored on the Appliance. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Appliance

- House the Appliance within a power and climate-controlled location that is appropriate for computer and IT storage equipment
- Connect the Appliance to the Client s server network
- Open any necessary ports and conduits between the Appliance and the servers to be backed up
- Open any necessary ports and conduits between the Appliances and OneNeck s ReliaCloud Location
- Assist with any Appliance repair or replacement as needed, and provide escorted access to the Appliance for OneNeck and/or OneNeck s authorized service vendor
- Install any associated software agents on servers or infrastructure to be backed up
- Return all Appliances to OneNeck within five (5) business days after the end of term
- Coordinate all Client responsibilities outlined herein, including all necessary communication to Client personnel
- Provide or purchase all necessary equipment, cabling, circuits, and other materials required for the services, unless OneNeck explicitly provides that such materials are included as part of the services
- Ensure compliance with any national or local safety standard or similar requirements affecting the installation of the Appliance
- Provide OneNeck with access, passwords, access codes or security devices as necessary to perform the services

Backup Operation

- Define backup content
- Define frequency, schedule, location, and retention of the backups
- Conduct operating system administration of servers subject to backup
- Validate data restored
- Install and manage backup clients on servers subject to backup if local agents are required
- Install any associated software clients (agents) on servers or infrastructure to be backed up

600609 ReliaCloud Backup Service for On-Prem. - 80 TB Appliance

Company's Responsibilities and Included Features

ReliaCloud Backup Service for On-Prem. 10 TB Appliance (Appliance) provides a local storage appliance for the purpose of facilitating backups with local storage capacity up to 10 terabytes (TB) of usable storage capacity. This service requires a subscription to Company-provided backup client licensing services.

A client refers to a software agent installed on the computer, physical or virtual server, or database to protect a specific type of data.

This service is delivered as a metered service allowing the Client to consume the storage in a pay-as-you-go model up to the maximum capacity of the Appliance (10 TB).

On-Premises Appliance

- Maintain ongoing support contracts for all hardware and software involved in the operation and support of the

Appliance
- Manage service capacity
- Monitor Appliance health
- Repair or replace (as necessary) equipment
- Maximum appliance storage capacity of 10TB usable
- Two (2) 10 Gb network ports

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup, and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their solution
  - General operating system level troubleshooting
  - Escalation to the software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This is a metered service.
- The size of the stored data is measured as the largest peak size in GB during the month stored on the Appliance. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Appliance

- House the Appliance within a power and climate-controlled location that is appropriate for computer and IT storage equipment
- Connect the Appliance to the Client s server network
- Open any necessary ports and conduits between the Appliance and the servers to be backed up
- Open any necessary ports and conduits between the Appliances and OneNeck s ReliaCloud Location
- Assist with any Appliance repair or replacement as needed, and provide escorted access to the Appliance for OneNeck and/or OneNeck s authorized service vendor
- Install any associated software agents on servers or infrastructure to be backed up
- Return all Appliances to OneNeck within five (5) business days after the end of term
- Coordinate all Client responsibilities outlined herein, including all necessary communication to Client personnel
- Provide or purchase all necessary equipment, cabling, circuits, and other materials required for the services, unless OneNeck explicitly provides that such materials are included as part of the services
- Ensure compliance with any national or local safety standard or similar requirements affecting the installation of the Appliance

- Provide OneNeck with access, passwords, access codes or security devices as necessary to perform the services

Backup Operation

- Define backup content
- Define frequency, schedule, location, and retention of the backups
- Conduct operating system administration of servers subject to backup
- Validate data restored
- Install and manage backup clients on servers subject to backup if local agents are required
- Install any associated software clients (agents) on servers or infrastructure to be backed up

600610 ReliaCloud Backup Service - Remote Pod Storage

Company's Responsibilities and Included Features

ReliaCloud Backup Service - Remote Pod Storage provides an auxiliary storage target for the purpose of facilitating backup storage at a secondary ReliaCloud Pod (site). This service requires a subscription to Company-provided backup client licensing services and one (1) of the following: Local Pod Storage Services, Cloud Direct, or On-Prem. Appliance services (separate Item IDs).

Service Metering

- This is a metered service.
- The size of the stored data is measured as the largest peak size in GB during the month stored within designated ReliaCloud Pod sites. Data stored equals the final amount of data stored on- disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Service Level Agreement (SLA)

- SLA for service availability is 100%

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Subscribe to ReliaCloud Backup Service for Local Pod Storage, Cloud Direct, or On-Prem. Appliance
- Subscribe to ReliaCloud Backup Client License service(s)

600613 ReliaCloud Backup Service - LTR via Microsoft Azure Block Blob Storage

Company's Responsibilities and Included Features

ReliaCloud Backup Service - LTR via Microsoft Azure Block Blob Storage leverages Client's Microsoft Azure subscription to access Microsoft Azure Block Blob storage services for Client configured policies that have Long Term Retention (LTR) storage requirements.

Company will:

- provide the transfer of protected data identified within a mutually agreed LTR policy to Microsoft Azure via Company s network;
- manage the transfer of the data and configuration of the associated Microsoft Azure services for this process; and
- provide support for:
    - access issues to Client s Microsoft Azure portal;
    - billing questions and disputes;
    - primary technical point of contact; and
    - necessary escalations of Microsoft Azure issues to Microsoft. Examples of operational or technical support issues that may be escalated include, but are not limited to, (i) undocumented problems with Microsoft Azure services that fail to operate in accordance with service descriptions, (ii) unavailable services, (iii) bugs and other irregularities that affect service appearance or operation, and (iv) large-scale network disruptions.

Actual charges will vary based upon Client's elections to the volume of data stored per month, quantity and types of operations performed, data transfer costs, and data redundancy option selected. Pricing, service and support descriptions, and features for the Microsoft Azure services are defined on Microsoft Azure's website (https://azure.microsoft.com) and are subject to the terms set forth in the separate Statement of Work for the Azure services (if purchased from Company) or Microsoft s terms and conditions (if purchased from Microsoft).

This service requires (i) the use of a ReliaCloud Backup storage service, local pod, remote pod, or an on-premises appliance (separate Item IDs); and (ii) a subscription to Company-provided backup client licensing services.

Service Metering

- This is a metered service and is based on the aggregate amount of all data transferred to Microsoft Azure from the Client backup operations. The billing period for this service is monthly, and data transferred is measured by the backup system. The unit of measurement is terabytes (TB) transferred rounded-up to the nearest whole TB.
- Service fees are applicable to data ingress to Microsoft Azure. There are no egress charges from Company.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Subscribe to Microsoft Azure services under a separate agreement through Company, or directly from Microsoft Azure
- Identify a storage account from Microsoft Azure
- Provide Company Client s Microsoft Azure subscription ID
- Provide Company use of Client s Microsoft Azure access key
- Subscribe to Microsoft Azure services, a separate agreement through Company, or directly from Microsoft Azure

Backup Operation

- Define backup content
- Define frequency, schedule, location and retention of the backups for data that requires long-term retention
- Conduct operating system administration of servers subject to backup
- Validate data restored
- Install and manage backup agents on servers subject to backup if local agents are required
- Install any associated software (agents) on servers or infrastructure to be backed up

600633 ReliaCloud Backup Service for On-Prem. - 20 TB Appliance

Company's Responsibilities and Included Features

ReliaCloud Backup Service for On-Prem. 20 TB Appliance (Appliance) provides a local storage appliance for the purpose of facilitating backups with local storage capacity of up to 20 terabytes (TB) of usable storage capacity. This service requires a subscription to Company-provided backup client licensing services.

A client refers to a software agent installed on the computer, physical or virtual server, or database to protect a specific type of data.

The service is delivered as a metered service allowing Client to consume the storage in a pay-as-you-go model up to the maximum capacity of the Appliance (20 TB).

On-Premises Appliance

- Maintain ongoing support contracts for all hardware and software involved in operation and support of the Appliance
- Manage service capacityMaintain and monitor Appliance health
- Repair or replace (as necessary) equipment
- Maximum appliance storage capacity of 80TB usable
- Two (2) 10Gb network ports

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
    - Policy definition
    - Backup job scheduling
    - Backup initiation
    - Restoration initiation
    - Data protection definition
    - Monitor backups and restores
    - Consumption reporting
- Provide support, setup, and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General operating system level troubleshooting
    - Escalation to the software provider
- To resolve system incidents, Company will:
    - Apply Company known solutions
    - Apply backup software vendor provided solutions
    - Document user issues and system errors
- Company will triage and manage the troubleshooting process for backup errors.

Service Metering

- This is a metered service.
- The size of the stored data is measured as the largest peak size in GB during the month stored on the Appliance. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Appliance

- House the Appliance within a power and climate-controlled location that is appropriate for computer and IT storage equipment
- Connect the Appliance to Client s server network
- Open any necessary ports and conduits between the Appliance and the servers to be backed up
- Open any necessary ports and conduits between the Appliance and OneNeck s ReliaCloud Location
- Assist with any Appliance repair or replacement as needed, and provide escorted access to the Appliance for OneNeck and/or OneNeck s authorized service vendor
- Install any associated software agents on servers or infrastructure to be backed up
- Return all Appliances to OneNeck within five (5) business days after the end of term
- Coordinate all Client responsibilities outlined herein, including all necessary communication to Client personnel
- Provide or purchase all necessary equipment, cabling, circuits, and other materials required for the services, unless OneNeck explicitly provides that such materials are included as part of the services
- Ensure compliance with any national or local safety standard or similar requirement affecting the installation of the Appliance
- Provide OneNeck with access, passwords, access codes or security devices as necessary to perform the services

Backup Operation

- Define backup content
- Define frequency, schedule, location, and retention of the backups
- Conduct operating system administration of servers subject to backup

- Validate data restored
- Install and manage backup clients on servers subject to backup if local agents are required
- Install any associated software clients (agents) on servers or infrastructure to be backed up

600634 ReliaCloud Backup Service for On-Prem. - 40 TB Appliance

Company's Responsibilities and Included Features

ReliaCloud Backup Service for On-Prem. 40 TB Appliance (Appliance) provides a local storage appliance for the purpose of facilitating backups with local storage capacity of up to 40 terabytes (TB) of usable storage capacity. This service requires a subscription to Company-provided backup client licensing services.

A client refers to a software agent installed on the computer, physical or virtual server, or database to protect a specific type of data.

The service is delivered as a metered service allowing Client to consume the storage in a pay-as-you-go model up to the maximum capacity of the Appliance (40 TB).

On-Premises Appliance

- Maintain ongoing support contracts for all hardware and software involved in operation and support of the Appliance
- Manage service capacityMaintain and monitor Appliance health
- Repair or replace (as necessary) equipment
- Maximum appliance storage capacity of 40TB usable
- Two (2) 10Gb network ports
- Two (2) FC HBA ports

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup, and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General operating system level troubleshooting
  - Escalation to the software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
  - Document user issues and system errors
- Company will triage and manage the troubleshooting process for backup errors.

Service Metering

- This is a metered service.

- The size of the stored data is measured as the largest peak size in GB during the month stored on the Appliance. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Appliance

- House the Appliance within a power and climate-controlled location that is appropriate for computer and IT storage equipment
- Connect the Appliance to Client s server network
- Open any necessary ports and conduits between the Appliance and the servers to be backed up
- Open any necessary ports and conduits between the Appliance and OneNeck s ReliaCloud Location
- Assist with any Appliance repair or replacement as needed, and provide escorted access to the Appliance for OneNeck and/or OneNeck s authorized service vendor
- Install any associated software agents on servers or infrastructure to be backed up
- Return all Appliances to OneNeck within five (5) business days after the end of term
- Coordinate all Client responsibilities outlined herein, including all necessary communication to Client personnel
- Provide or purchase all necessary equipment, cabling, circuits, and other materials required for the services, unless OneNeck explicitly provides that such materials are included as part of the services
- Ensure compliance with any national or local safety standard or similar requirement affecting the installation of the Appliance
- Provide OneNeck with access, passwords, access codes or security devices as necessary to perform the services

Backup Operation

- Define backup content
- Define frequency, schedule, location, and retention of the backups
- Conduct operating system administration of servers subject to backup
- Validate data restored
- Install and manage backup clients on servers subject to backup if local agents are required
- Install any associated software clients (agents) on servers or infrastructure to be backed up

601447 ReliaCloud Backup Service for On-Prem. - 60 TB Appliance

Company's Responsibilities and Included Features

ReliaCloud Backup Service for On-Prem. 60 TB Appliance (Appliance) provides a local storage appliance for the purpose of facilitating backups with local storage capacity of up to 60 terabytes (TB) of usable storage capacity. This service requires a subscription to Company-provided backup client licensing services.

A client refers to a software agent installed on the computer, physical or virtual server, or database to protect a specific type of data.

The service is delivered as a metered service allowing Client to consume the storage in a pay-as-you-go model up to the maximum capacity of the Appliance (60 TB).

On-Premises Appliance

- Maintain ongoing support contracts for all hardware and software involved in operation and support of the Appliance
- Manage service capacityMaintain and monitor Appliance health
- Repair or replace (as necessary) equipment
- Maximum appliance storage capacity of 60TB usable
- Two (2) 10Gb network ports

- Two (2) FC HBA ports

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup, and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General operating system level troubleshooting
  - Escalation to the software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
  - Document user issues and system errors
- Company will triage and manage the troubleshooting process for backup errors.

Service Metering

- This is a metered service.
- The size of the stored data is measured as the largest peak size in GB during the month stored on the Appliance. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Appliance

- House the Appliance within a power and climate-controlled location that is appropriate for computer and IT storage equipment
- Connect the Appliance to Client s server network
- Open any necessary ports and conduits between the Appliance and the servers to be backed up
- Open any necessary ports and conduits between the Appliance and OneNeck s ReliaCloud Location
- Assist with any Appliance repair or replacement as needed, and provide escorted access to the Appliance for OneNeck and/or OneNeck s authorized service vendor
- Install any associated software agents on servers or infrastructure to be backed up
- Return all Appliances to OneNeck within five (5) business days after the end of term
- Coordinate all Client responsibilities outlined herein, including all necessary communication to Client personnel
- Provide or purchase all necessary equipment, cabling, circuits, and other materials required for the services, unless OneNeck explicitly provides that such materials are included as part of the services
- Ensure compliance with any national or local safety standard or similar requirement affecting the installation of the Appliance
- Provide OneNeck with access, passwords, access codes or security devices as necessary to perform the services

Backup Operation

- Define backup content
- Define frequency, schedule, location, and retention of the backups
- Conduct operating system administration of servers subject to backup
- Validate data restored
- Install and manage backup clients on servers subject to backup if local agents are required
- Install any associated software clients (agents) on servers or infrastructure to be backed up

601530 ReliaCloud Backup Service - Primary Copy Storage

Company's Responsibilities and Included Features

ReliaCloud Backup Service Primary Copy Storage provides the primary storage target for backup storage within a ReliaCloud site. The primary copy is defined as the first copy of data made from the backup operation.

Supported Deployments

This Service supports the following service environments:

- ReliaCloud Service - Primary backup jobs initiated from within ReliaCloud to its data center of origin
- Colocation Service - Primary backup jobs initiated from Company s colocation space to that colocation site s local storage
- Cloud Direct Service - Primary backup job initiated from the Client s remote locations, such as remote and branch offices, where the maximum amount of aggregate front-end protected data size is less than five (5) terabytes (TB), and a ReliaCloud On-prem backup appliance is not deployed at that remote location.
    - "Front-end protected data means the amount of application data to be protected that is stored on Client s server(s)

Service Metering

- This is a metered service.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored within designated ReliaCloud pod sites. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Service Connectivity

The following connectivity solutions and requirements are described below:

- Colocation Service - This Service is provided to the colocation environment to a single demarcation within Client's colocation infrastructure and is delivered over a Cat6 ethernet cable as part of a Backup Area Network (BAN).
- Cloud Direct Service This Service runs over the Internet, and requires the Client have Internet services available where the infrastructure to be protected resides..

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Required Company Services

- Maintain a current subscription to one or more Company provided ReliaCloud backup Client license service(s).

Service Connectivity

- For Colocation Service:
    - Provide a network port to terminate the Company's Cat6 ethernet connection
    - Design and implement a network security policy between Client's network and Company's BAN
- For Cloud Direct Service:

- Maintaining an internet or wide area network (WAN) connection with sufficient size and available capacity to facilitate Company s backup and restoration processes
- Appropriate sizing of the internet or WAN connection to successfully complete backup and restoration operations
- Opening any necessary ports and conduits between Client s servers subject to backup and the ReliaCloud Backup Service Primary Copy Storage Backup Operation

Backup Operation

- Define backup content
- Define frequency, schedule, location, and retention of the backups for data that requires long-term retention
- Conduct operating system administration of servers subject to backup
- Validate data restored
- Install and manage backup agents on servers subject to backup if local agents are required
- Install any associated software (agents) on servers or infrastructure to be backed up

601531 ReliaCloud Backup Service - Additional Copy Storage

Company's Responsibilities and Included Features

ReliaCloud Backup Service Additional Copy Storage provides a storage target for backup storage at a secondary ReliaCloud site. The primary copy is defined as the first copy of data made from the backup operation. The additional copy is any copy/copies other than the primary copy.

Service Metering

- This is a metered service.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored within designated ReliaCloud pod sites. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Subscriptions

- Maintain a current subscription to one or more ReliaCloud Backup Client License service(s).
- Maintain a current subscription to Company s ReliaCloud Backup Service - Primary Copy Storage or On-Prem Appliance Services

603820 VM & Kubernetes Standard Data Protection by Commvault Metallic (Hypervisor) - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect virtual machine & Kubernetes data for enrolled VMs. Backups are done at the hypervisor level and no agent is required. Individual files can be restored.

This service requires the use of the Metallic Recovery Reserve Azure Hot Storage and Metallic Recovery Reserve Azure Cool Storage.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation

Restoration initiation
    - Data protection definition
    - Monitor backups and restores
    - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Microsoft Online Services level troubleshooting
    - Escalation to software provider
- To resolve system incidents, Company will:
    - Apply Company known solutions
    - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number unique clients of this type (VM based) that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is per VM.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic VM and Kubernetes Backup - Standard for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

603821 VM & Kubernetes Advanced Data Protection by Commvault Metallic (Hypervisor, File, Agent, IaaS Database - MS SQL, Oracle) - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect virtual machine & Kubernetes data for enrolled VMs using a Company-provided backup software agent. Agent allows for backup and data protection down to the file level and supports backup of Microsoft SQL and Oracle database applications running on the virtual machine.

This service requires the use of the Metallic Recovery Reserve Azure Hot Storage and Metallic Recovery Reserve Azure Cool Storage.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions

Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number unique clients of this type (VM based) that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is per VM.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic VM and Kubernetes Backup - Advanced for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

603822 VM & Kubernetes Enterprise Data Protection by Commvault Metallic (Hypervisor, File, Agent, IaaS Database - Oracle RAC, SAP) - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect virtual machine & Kubernetes data for enrolled VMs using a Company-provided backup software agent. Agent allows for backup and data protection down to the file level and supports backup of Microsoft SQL and Oracle database applications running on the virtual machine. Oracle RAC and SAP IaaS database applications running the virtual machine are also supported.

This service requires the use of the Metallic Recovery Reserve Azure Hot Storage and Metallic Recovery Reserve Azure Cool Storage.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number unique clients of this type (VM based) that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is per VM.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic VM and Kubernetes Backup - Enterprise for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement

located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.

- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

603823 File & Object Data Protection by Commvault Metallic - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect large file services on virtual machines, Azure Files and Azure blob storage.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:

Policy definition
    - Backup job scheduling
    - Backup initiation
    - Restoration initiation
    - Data protection definition
    - Monitor backups and restores
    - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Microsoft Online Services level troubleshooting
    - Escalation to software provider
- To resolve system incidents, Company will:
    - Apply Company known solutions
    - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The amount of storage protected is determined by the largest peak size in gigabytes (GB) protected GB of storage that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB Protected or front-end TB (FET).

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic File & Object Backup for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

603824 Endpoint Data Protection by Commvault Metallic Tier 1 - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect supported Endpoint device data.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Endpoint Backup Essentials for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

Provide Company access to Microsoft Online Services and Azure Resources

603825 Microsoft 365 Enterprise Data Protection by Commvault Metallic Tier 1 - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint Online, Microsoft Teams, Microsoft Project) for enrolled users.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

603827 Endpoint eDiscovery Data Protection by Commvault Metallic Tier 1 - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to enable searching and exporting data for legal hold and Electronic Discovery Reference Model (EDRM) compliance.

This service requires the use of the ItemID 603824 Endpoint Data Protection by Commvault Metallic.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition

Monitor backups and restores
    - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Microsoft Online Services level troubleshooting
    - Escalation to software provider
- To resolve system incidents, Company will:
    - Apply Company known solutions
    - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for eDiscovery which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Endpoint Backup eDiscovery Edition for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

603828 Recovery Reserve Azure Hot Storage USCAN Data Protection by Commvault Metallic - 1 Month (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Azure virtual machine backups

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Provider, Azure Hot Tier, USACAN (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request

support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

603829 Recovery Reserve Azure Cool Storage USCAN Data Protection by Commvault Metallic - 1 Month (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Azure virtual machine backups.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Provider, Azure Cool Tier, USACAN (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at

https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

603933 Database PaaS Data Protection by Commvault Metallic (Cloud Native and Enterprise) - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect supported cloud native (PaaS) and enterprise database applications.

Storage is included in this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:

        - Policy definition
        - Backup job scheduling
        - Backup initiation
        - Restoration initiation
        - Data protection definition
        - Monitor backups and restores
        - Consumption reporting
    - Provide support, setup and configuration of backup policies (as requested by Client)
    - Provide support for initiation of backups and restorations (as requested by Client)
    - Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Microsoft Online Services level troubleshooting
    - Escalation to software provider
- To resolve system incidents, Company will:
    - Apply Company known solutions
    - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The amount of storage protected is determined by the largest peak size in gigabytes (GB) protected GB of storage that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB Protected or front-end TB (FET).

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Database Backup for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604137 ReliaCloud Backup Commvault IntelliSnap Integration Management

Definitions

IntelliSnap: Commvault IntelliSnap (IntelliSnap) technology automates and orchestrates snapshot management for storage arrays. Storage arrays host the data for virtual machines, applications, and data that resides on physical servers and hypervisor hosts.

Backup Client: (BU Client) The entity that is to be backed up such as a VM, file service, or physical server.

Day-Two Support: Support services that start after the completion of an implementation project.

Company's Responsibilities and Included Features

ReliaCloud Backup Commvault IntelliSnap Integration Management (Service) provides integration, licensing enablement, and management of the IntelliSnap feature within the ReliaCloud Backup service platform. The Service allows for the integration of physical storage arrays, hypervisors, and cloud storage platforms to leverage their native snapshot capabilities to improve backup life-cycle operations.

The Service is an add-on option to the existing ReliaCloud Backup service platform and requires subscription of the following base services:

- ReliaCloud Backup Client License for Hypervisor Backup
- ReliaCloud Backup Client License for Hypervisor / File System Backup
- ReliaCloud Backup Client License for Hypervisor / File System / Application Backup

Depending upon deployment options a combination of some or all of the following services:

- ReliaCloud Backup Service Primary Copy Storage
- ReliaCloud Backup Service Additional Copy Storage
- ReliaCloud Backup Service On prem. Appliances

Use of the IntelliSnap feature set requires Company approved compatibility and may additionally require application vendor approved compatibility and application vendor access codes, and or drivers.

Service Initiation

Use of the Service requires a professional services engagement to conduct initial deployment and integration of the infrastructure elements. Day-Two Support, and on-going management starts after the completion of Service Initiation.

Management

Company will provide Day-two Support and management of the following IntelliSnap functions:

- Server plans
- Backup destinations
- Backup retention rules
- Backup schedule as defined by the Client
- Backup content parameters set exclude operations as defined by the Client
- Snapshot operations (if applicable and compatible)
    - IntelliSnap Instant clone for applications
    - IntelliSnap support for Live Mount
    - IntelliSnap support for Live VM Recovery
    - Mounting and unmounting snapshots
    - Deleting snapshots
    - Reverting snapshots
    - Snap pruning
    - Snap reconciliation
- SCSI reservation
- Replication
    - Requires contracting to ReliaCloud Backup Service Additional Copy Storage, or to one of the ReliaCloud Backup Service for On-Prem. Appliance.

Incident Triage and Troubleshooting

Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:

- Company knowledge of known errors and their potential solutions
- General operating system level troubleshooting
- Escalation to software provider
- To resolve system incidents, Company will:
    - Apply Company known solutions
    - Apply backup software vendor provided solutions
    - Document user issues and system errors

Service Metering

This is a metered service.

- The unit of measure is per BU Client
- The number of BU Clients is determined by the number of unique BU Clients leveraging the Service within the billing period.
- The billing period for this service is monthly, as measured by the backup system.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Service Implementation

Client must contract with Company for a separate Professional Services engagement to turn-up the Service.

Storage Array Integration Assistance

- If applicable provide credentials for the physical storage array, or credentials for the virtualized data stores.
- Protected array must be compatible with Commvault software for IntelliSnap backups. Documentation can be found at https://documentation.commvault.com
- Management and support of the protected storage array
- Provide licensing that may be required by the protected array s vendor to leverage the IntelliSnap feature set.
- Provide licensing and support codes, and drivers from the application vendor if applicable
- Provider storage network and protocol support and troubleshooting
- Provide two (2) storage network connections to Company backup appliance if applicable

Application Restoration

Client is responsible for the restoration or reinstallation and configuration application software

Define Backup Content

Define frequency, schedule, location, and retention of the backups

- Conduct operating system administration of servers subject to backup
- Validate data restored

Subscriptions

- Maintain a current subscription to one or more ReliaCloud Backup Client License service(s).
- Maintain a current subscription to Company s ReliaCloud Backup Service - Primary Copy Storage or On-Prem Appliance Services

604370 Recovery Reserve Azure Hot Storage APJ Data Protection by Commvault Metallic - 1 Month (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the primary storage target for Azure virtual machine backups. The primary copy is defined as the first copy of data made from the backup operation.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Provider, Azure Hot Tier, APJ (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604371 Recovery Reserve Azure Cool Storage APJ Data Protection by Commvault Metallic - 1 Month (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Azure virtual machine backups.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Provider, Azure Cool

Tier, APJ (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.

- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604372 Recovery Reserve Azure Hot Storage EMEA Data Protection by Commvault Metallic - 1 Month (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the primary storage target for Azure virtual machine backups. The primary copy is defined as the first copy of data made from the backup operation.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Provider, Azure Hot Tier, EMEA (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604373 Recovery Reserve Azure Cool Storage EMEA Data Protection by Commvault Metallic - 1 Month (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long-term retention storage target for Azure virtual machine backups.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Provider, Azure Cool Tier, EMEA (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

  Expert User Technical Support*

  Technical support may only be requested by a Client Expert User*, available during the following hours:

  -
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

  * An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal

- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604374 Microsoft 365 Enterprise with eDiscovery Data Protection by Commvault Metallic Tier 1 - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint, Teams) for enrolled users. eDiscovery to enable searching and exporting data for legal hold and Electronic Discovery Reference Model (EDRM) compliance is included.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

This service is delivered as a metered service allowing Client to consume managed software licensing.

- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise with eDiscovery for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604375 Microsoft 365 Standard Data Protection by Commvault Metallic Tier 1 - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint Online, Microsoft Teams, Microsoft Project) for enrolled users.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604376 Microsoft Dynamics 365 Data Protection by Commvault Metallic - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Dynamics 365 Production and Sandbox environments (Sales CRM, Marketing CRM, Customer Service CRM, Field Service CRM)

This service includes target backup storage.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
    - Policy definition
    - Backup job scheduling
    - Backup initiation
    - Restoration initiation
    - Data protection definition
    - Monitor backups and restores

        - Consumption reporting
    - Provide support, setup and configuration of backup policies (as requested by Client)
    - Provide support for initiation of backups and restorations (as requested by Client)
    - Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Microsoft Online Services level troubleshooting
    - Escalation to software provider
- To resolve system incidents, Company will:
    - Apply Company known solutions
    - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft Dynamics 365 for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal

- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604378 Salesforce Data Protection by Commvault Metallic - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Salesforce Production and Sandbox environments (Financial Cloud, Health Cloud, Sales Cloud, Service Cloud). Supported editions Lightning Developer, Lightning Performance, Lightning Enterprise, Lightning Unlimited

This service includes target backup storage.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a

month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Salesforce for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604405 Storage for SaaS Apps Data Protection by Commvault Metallic - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to to provide additional storage for SaaS apps.

Applicable to ItemID 603825, 604374, and 604375.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The amount of GB is determined by the largest peak size in gigabytes (GB) protected of storage that are active within a month minus the allotted protected storage of the SaaS app ItemIDs. If the largest peak size is greater than the allotted storage, the remainder is the quantity for this ItemID (rounded up to the nearest GB). The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Storage for SaaS Apps for Service Providers (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604420 Microsoft 365 Enterprise Data Protection by Commvault Metallic Tier 2 - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint Online, Microsoft Teams, Microsoft Project) for enrolled users.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions

available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.

- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604421 Microsoft 365 Standard Data Protection by Commvault Metallic Tier 2 - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint Online, Microsoft Teams, Microsoft Project) for enrolled users.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:

- Policy definition
- Backup job scheduling
- Backup initiation
- Restoration initiation
- Data protection definition
- Monitor backups and restores
- Consumption reporting

- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604422 Microsoft 365 Enterprise with eDiscovery Data Protection by Commvault Metallic Tier 2 - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint, Teams) for enrolled users. eDiscovery to enable searching and exporting data for legal hold and Electronic Discovery Reference Model (EDRM) compliance is included.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting

        - Escalation to software provider
    - To resolve system incidents, Company will:
        - Apply Company known solutions
        - Apply backup software vendor provided solutions
    - Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise with eDiscovery for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604423 Microsoft 365 Enterprise Data Protection by Commvault Metallic Tier 3 - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint Online, Microsoft Teams, Microsoft Project) for enrolled users.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions

available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.

- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604424 Microsoft 365 Standard Data Protection by Commvault Metallic Tier 3 - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint Online, Microsoft Teams, Microsoft Project) for enrolled users.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:

- Policy definition
- Backup job scheduling
- Backup initiation
- Restoration initiation
- Data protection definition
- Monitor backups and restores
- Consumption reporting

- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604425 Microsoft 365 Enterprise with eDiscovery Data Protection by Commvault Metallic Tier 3 - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint, Teams) for enrolled users. eDiscovery to enable searching and exporting data for legal hold and Electronic Discovery Reference Model (EDRM) compliance is included.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting

        - Escalation to software provider
    - To resolve system incidents, Company will:
        - Apply Company known solutions
        - Apply backup software vendor provided solutions
    - Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise with eDiscovery for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604517 Database PaaS Data Protection by Commvault Metallic (Cloud Native and Enterprise) - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect supported cloud native (PaaS) and enterprise database applications.

Storage is included in this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The amount of storage protected is determined by the largest peak size in gigabytes (GB) protected GB of storage that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB Protected or front-end TB (FET).

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Database Backup for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject

to change as determined by Commvault.

- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604518 Endpoint Data Protection by Commvault Metallic Tier 1 - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect supported Endpoint device data.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
    - Policy definition
    - Backup job scheduling
    - Backup initiation
    - Restoration initiation
    - Data protection definition
    - Monitor backups and restores
    - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Microsoft Online Services level troubleshooting
    - Escalation to software provider
- To resolve system incidents, Company will:
    - Apply Company known solutions
    - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Endpoint Backup Essentials for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604519 Endpoint eDiscovery Data Protection by Commvault Metallic Tier 1 - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to enable searching and exporting data for legal hold and Electronic Discovery Reference Model (EDRM) compliance.

This service requires the use of the ItemID 603824 Endpoint Data Protection by Commvault Metallic.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions

        - Apply backup software vendor provided solutions
    - Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for eDiscovery which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Endpoint Backup eDiscovery Edition for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604520 File & Object Data Protection by Commvault Metallic - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect large file services on virtual machines, Azure Files and Azure blob storage.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The amount of storage protected is determined by the largest peak size in gigabytes (GB) protected GB of storage that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB Protected or front-end TB (FET).

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic File & Object Backup for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604521 Microsoft 365 Enterprise Data Protection by Commvault Metallic Tier 1 - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint Online, Microsoft Teams, Microsoft Project) for enrolled users.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation

        - Data protection definition
        - Monitor backups and restores
        - Consumption reporting
    - Provide support, setup and configuration of backup policies (as requested by Client)
    - Provide support for initiation of backups and restorations (as requested by Client)
    - Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Microsoft Online Services level troubleshooting
    - Escalation to software provider
- To resolve system incidents, Company will:
    - Apply Company known solutions
    - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604522 Microsoft 365 Enterprise Data Protection by Commvault Metallic Tier 2 - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint Online, Microsoft Teams, Microsoft Project) for enrolled users.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.

- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint Online, Microsoft Teams, Microsoft Project) for enrolled users.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents

6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604524 Microsoft 365 Enterprise with eDiscovery Data Protection by Commvault Metallic Tier 1 - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint, Teams) for enrolled users. eDiscovery to enable searching and exporting data for legal hold and Electronic Discovery Reference Model (EDRM) compliance is included.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores

Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise with eDiscovery for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604525 Microsoft 365 Enterprise with eDiscovery Data Protection by Commvault Metallic Tier 2 - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint, Teams) for enrolled users. eDiscovery to enable searching and exporting data for legal hold and Electronic Discovery Reference Model (EDRM) compliance is included.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise with eDiscovery for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604526 Microsoft 365 Enterprise with eDiscovery Data Protection by Commvault Metallic Tier 3 - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint, Teams) for enrolled users. eDiscovery to enable searching and exporting data for legal hold and Electronic Discovery Reference Model (EDRM) compliance is included.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise with eDiscovery for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604527 Microsoft 365 Standard Data Protection by Commvault Metallic Tier 1 - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint Online, Microsoft Teams, Microsoft Project) for enrolled users.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation

        - Restoration initiation
        - Data protection definition
        - Monitor backups and restores
        - Consumption reporting
    - Provide support, setup and configuration of backup policies (as requested by Client)
    - Provide support for initiation of backups and restorations (as requested by Client)
    - Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Microsoft Online Services level troubleshooting
    - Escalation to software provider
- To resolve system incidents, Company will:
    - Apply Company known solutions
    - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604528 Microsoft 365 Standard Data Protection by Commvault Metallic Tier 2 - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint Online, Microsoft Teams, Microsoft Project) for enrolled users.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604529 Microsoft 365 Standard Data Protection by Commvault Metallic Tier 3 - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint Online, Microsoft Teams, Microsoft Project) for enrolled users.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604530 Microsoft Dynamics 365 Data Protection by Commvault Metallic - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Dynamics 365 Production and Sandbox environments (Sales CRM, Marketing CRM, Customer Service CRM, Field Service CRM)

This service includes target backup storage.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
    - Policy definition
    - Backup job scheduling
    - Backup initiation
    - Restoration initiation

        - Data protection definition
        - Monitor backups and restores
        - Consumption reporting
    - Provide support, setup and configuration of backup policies (as requested by Client)
    - Provide support for initiation of backups and restorations (as requested by Client)
    - Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Microsoft Online Services level troubleshooting
    - Escalation to software provider
- To resolve system incidents, Company will:
    - Apply Company known solutions
    - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft Dynamics 365 for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604531 Recovery Reserve Azure Cool Storage APJ Data Protection by Commvault Metallic - 1 Year (Annual)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Azure virtual machine backups.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Provider, Azure Cool Tier, APJ (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request

support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604532 Recovery Reserve Azure Cool Storage EMEA Data Protection by Commvault Metallic - 1 Year (Annual)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long-term retention storage target for Azure virtual machine backups.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Provider, Azure Cool Tier, EMEA (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604533 Recovery Reserve Azure Cool Storage USCAN Data Protection by Commvault Metallic - 1 Year (Annual)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Azure virtual machine backups.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The

billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Provider, Azure Cool Tier, USACAN (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604534 Recovery Reserve Azure Hot Storage APJ Data Protection by Commvault Metallic - 1 Year (Annual)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the primary

storage target for Azure virtual machine backups. The primary copy is defined as the first copy of data made from the backup operation.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Provider, Azure Hot Tier, APJ (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal

Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604535 Recovery Reserve Azure Hot Storage EMEA Data Protection by Commvault Metallic - 1 Year (Annual)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the primary storage target for Azure virtual machine backups. The primary copy is defined as the first copy of data made from the backup operation.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Provider, Azure Hot Tier, EMEA (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604536 Recovery Reserve Azure Hot Storage USCAN Data Protection by Commvault Metallic - 1 Year (Annual)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Azure virtual machine backups

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Provider, Azure Hot Tier, USACAN (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604537 Salesforce Data Protection by Commvault Metallic - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Salesforce Production and Sandbox environments (Financial Cloud, Health Cloud, Sales Cloud, Service Cloud). Supported editions Lightning Developer, Lightning Performance, Lightning Enterprise, Lightning Unlimited

This service includes target backup storage.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Salesforce for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604539 VM & Kubernetes Advanced Data Protection by Commvault Metallic (Hypervisor, File, Agent, IaaS Database - MS SQL, Oracle) - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect virtual machine & Kubernetes data for enrolled VMs using a Company-provided backup software agent. Agent allows for backup and data protection down to the file level and supports backup of Microsoft SQL and Oracle database applications running on the virtual machine.

This service requires the use of the Metallic Recovery Reserve Azure Hot Storage and Metallic Recovery Reserve Azure Cool Storage.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number unique clients of this type (VM based) that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is per VM.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic VM and Kubernetes Backup - Advanced for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604540 VM & Kubernetes Enterprise Data Protection by Commvault Metallic (Hypervisor, File, Agent, IaaS Database - Oracle RAC, SAP) - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect virtual machine & Kubernetes data for enrolled VMs using a Company-provided backup software agent. Agent allows for backup and data protection down to the

file level and supports backup of Microsoft SQL and Oracle database applications running on the virtual machine. Oracle RAC and SAP IaaS database applications running the virtual machine are also supported.

This service requires the use of the Metallic Recovery Reserve Azure Hot Storage and Metallic Recovery Reserve Azure Cool Storage.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number unique clients of this type (VM based) that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is per VM.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic VM and Kubernetes Backup - Enterprise for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604541 VM & Kubernetes Standard Data Protection by Commvault Metallic (Hypervisor) - 1 Year (Annual)

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect virtual machine & Kubernetes data for enrolled VMs. Backups are done at the hypervisor level and no agent is required. Individual files can be restored.

This service requires the use of the Metallic Recovery Reserve Azure Hot Storage and Metallic Recovery Reserve Azure Cool Storage.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting

- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Microsoft Online Services level troubleshooting
    - Escalation to software provider
- To resolve system incidents, Company will:
    - Apply Company known solutions
    - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number unique clients of this type (VM based) that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is per VM.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic VM and Kubernetes Backup - Standard for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content

- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604667 Microsoft 365 Enterprise with eDiscovery Data Protection by Commvault Metallic Tier 3 - 1 Year (Monthly) - Flowserve

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint, Teams) for enrolled users. eDiscovery to enable searching and exporting data for legal hold and Electronic Discovery Reference Model (EDRM) compliance is included.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.

The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise with eDiscovery for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604668 Microsoft 365 Enterprise with eDiscovery Data Protection by Commvault Metallic Tier 3 - 1 Month (Monthly) - Flowserve

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint, Teams) for enrolled users. eDiscovery to enable searching and exporting data for legal hold and Electronic Discovery Reference Model (EDRM) compliance is included.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise with eDiscovery for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604671 Microsoft 365 Enterprise with eDiscovery Data Protection by Commvault Metallic Tier 3 - 1 Year (Monthly) - Lozier

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint, Teams) for enrolled users. eDiscovery to enable searching and exporting data for legal hold and Electronic Discovery Reference Model (EDRM) compliance is included.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
    - Policy definition

Backup job scheduling
    - Backup initiation
    - Restoration initiation
    - Data protection definition
    - Monitor backups and restores
    - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Microsoft Online Services level troubleshooting
    - Escalation to software provider
- To resolve system incidents, Company will:
    - Apply Company known solutions
    - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise with eDiscovery for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604672 Microsoft 365 Enterprise with eDiscovery Data Protection by Commvault Metallic Tier 3 - 1 Month (Monthly) - Lozier

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint, Teams) for enrolled users. eDiscovery to enable searching and exporting data for legal hold and Electronic Discovery Reference Model (EDRM) compliance is included.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions

    - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise with eDiscovery for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604673 Microsoft 365 Enterprise Data Protection by Commvault Metallic Tier 3 - 1 Year (Monthly) - PDG

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint Online, Microsoft Teams, Microsoft Project) for enrolled users.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

604674 Microsoft 365 Enterprise Data Protection by Commvault Metallic Tier 3 - 1 Month (Monthly) PDG

This service leverages the Metallic offering from Commvault https://metallic.io/ to protect Microsoft Online Services data (Exchange Online, OneDrive, SharePoint Online, Microsoft Teams, Microsoft Project) for enrolled users.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
-
    - Policy definition
    - Backup job scheduling

Backup initiation
    - Restoration initiation
    - Data protection definition
    - Monitor backups and restores
    - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Microsoft Online Services level troubleshooting
    - Escalation to software provider
- To resolve system incidents, Company will:
    - Apply Company known solutions
    - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number of unique users enrolled for backups which are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is Per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Backup for Microsoft 365 Enterprise for Service Provider licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

606864 Recovery Reserve OCI Infrequent Access Storage APJ Data Protection by Commvault Metallic - 1 Month (Monthly)

This service leverages the Metallic Recovery ReserveTM offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Infrequent Access Tier, APJ (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents

- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

606865 Recovery Reserve OCI Infrequent Access Storage APJ Data Protection by Commvault Metallic - 1 Year (Annual)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Infrequent Access Tier, Upfront, APJ (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault

Systems, Inc and may be subject to change as determined by Commvault.

- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

606866 Recovery Reserve OCI Infrequent Access Storage APJ Data Protection by Commvault Metallic - 1 Year (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Infrequent Access Tier, Upfront, APJ (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

606867 Recovery Reserve OCI Standard Storage APJ Data Protection by Commvault Metallic - 1 Month (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Standard Tier, APJ (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal

- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

606868 Recovery Reserve OCI Standard Storage APJ Data Protection by Commvault Metallic - 1 Year (Annual)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Standard Tier, Upfront, APJ (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client

staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

606869 Recovery Reserve OCI Standard Storage APJ Data Protection by Commvault Metallic - 1 Year (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Standard Tier, Upfront, APJ (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.

- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

606870 Recovery Reserve OCI Infrequent Access Storage EMEA Data Protection by Commvault Metallic - 1 Month (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The

billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Infrequent Access Tier, EMEA (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

Year (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Infrequent Access Tier, Upfront, EMEA (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

606872 Recovery Reserve OCI Infrequent Access Storage EMEA Data Protection by Commvault Metallic - 1 Year (Annual)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Infrequent Access Tier, Upfront, EMEA (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

606873 Recovery Reserve OCI Standard Storage EMEA Data Protection by Commvault Metallic - 1 Month (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Standard Tier, EMEA (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

606874 Recovery Reserve OCI Standard Storage EMEA Data Protection by Commvault Metallic - 1 Year (Annual)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Standard Tier, Upfront, EMEA (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

606875 Recovery Reserve OCI Standard Storage EMEA Data Protection by Commvault Metallic - 1 Year (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term

retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Standard Tier, Upfront, EMEA (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal

Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

606876 Recovery Reserve OCI Infrequent Access Storage USCAN Data Protection by Commvault Metallic - 1 Month (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Infrequent Access Tier, USCAN (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

606877 Recovery Reserve OCI Infrequent Access Storage USCAN Data Protection by Commvault Metallic - 1 Year (Annual)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Infrequent Access Tier, Upfront, USCAN (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-

24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

606878 Recovery Reserve OCI Infrequent Access Storage USCAN Data Protection by Commvault Metallic - 1 Year (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI

Infrequent Access Tier, Upfront, USCAN (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.

- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

606879 Recovery Reserve OCI Standard Storage USCAN Data Protection by Commvault Metallic - 1 Month (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Standard Tier, USCAN (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

606880 Recovery Reserve OCI Standard Storage USCAN Data Protection by Commvault Metallic - 1 Year (Annual)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Standard Tier, Upfront, USCAN (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

606881 Recovery Reserve OCI Standard Storage USCAN Data Protection by Commvault Metallic - 1 Year (Monthly)

This service leverages the Metallic Recovery Reserve offering from Commvault https://metallic.io/ to provide the long term retention storage target for Oracle Cloud Infrastructure backup.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Metallic Recovery Reserve for Service Providers, OCI Standard Tier, Upfront, USCAN (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to OCI Resources

611270 File & Object Data Protection by Commvault Cloud - 1 Year (Monthly) Flowserve

This service leverages the Metallic offering from Commvault Cloud https://metallic.io/ to protect large file services on virtual machines, Azure Files and Azure blob storage.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The amount of storage protected is determined by the largest peak size in gigabytes (GB) protected GB of storage that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB Protected or front-end TB (FET).

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Backup & Recovery for Files & Objects for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611327 Database PaaS Data Protection by Commvault Cloud (Cloud Native and Enterprise) - 1 Year (Monthly) Flowserve

This service leverages the Metallic offering from Commvault Cloud https://metallic.io/ to protect supported cloud native (PaaS) and enterprise database applications.

Storage is included in this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The amount of storage protected is determined by the largest peak size in gigabytes (GB) protected GB of storage that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB Protected or front-end TB (FET).

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Backup & Recovery for Databases for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611328 VM & Kubernetes Data Protection by Commvault Cloud - 1 Year (Monthly) Flowserve

This service leverages the Metallic offering from Commvault Cloud https://metallic.io/ to protect virtual machine & Kubernetes data for enrolled VMs using a Company-provided backup software agent. Agent allows for backup and data protection down to the file level and supports backup of Microsoft SQL and Oracle database applications running on the virtual machine. Oracle RAC and SAP IaaS database applications running the virtual machine are also supported.

This service requires the use of the Metallic Air Gap Protect Azure Hot Storage and Metallic Air Gap Protect Azure Cool Storage.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number unique clients of this type (VM based) that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is per VM.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Backup & Recovery for VM for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further

provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611329 Active Directory Data Protection by Commvault Cloud (Active Directory, Azure Active Directory) - 1 Year (Monthly) Flowserve

This service leverages the Metallic offering from Commvault Cloud https://metallic.io/ to protect active directory data for enrolled users using a Company-provided backup software agent. Agent allows for backup and data protection and supports Active Directory and Azure Active Directory.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number unique clients of this type (User based) that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Backup & Recovery for Active Directory for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup

Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611335 Air Gap Protect Azure Cool Storage USCAN Data Protection by Commvault Cloud - 1 Year (Monthly) Flowserve

This service leverages the Metallic Air Gap Protect offering from Commvault Cloud https://metallic.io/ to provide the long term retention storage target for Azure virtual machine backups.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Air Gap Protect for Service Providers, US & Canada, Azure Cool Tier (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611336 Air Gap Protect Azure Hot Storage USCAN Data Protection by Commvault Cloud - 1 Year (Monthly) Flowserve

This service leverages the Metallic Air Gap Protect offering from Commvault Cloud https://metallic.io/ to provide the long term retention storage target for Azure virtual machine backups

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Air Gap Protect for Service Providers, US & Canada, Azure Hot Tier (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611337 Air Gap Protect Azure Cool Storage EMEA Data Protection by Commvault Cloud - 1 Year (Monthly) Flowserve

This service leverages the Metallic Air Gap Protect offering from Commvault Cloud https://metallic.io/ to provide the long-term retention storage target for Azure virtual machine backups.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Air Gap Protect for Service Providers, EMEA, Azure Cool Tier (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611338 Air Gap Protect Azure Hot Storage EMEA Data Protection by Commvault Cloud - 1 Year (Monthly) Flowserve

This service leverages the Metallic Air Gap Protect offering from Commvault Cloud https://metallic.io/ to provide the long-term retention storage target for Azure virtual machine backups.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Air Gap Protect for Service Providers, EMEA, Azure Hot Tier (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal

- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611339 Air Gap Protect Azure Cool Storage APJ Data Protection by Commvault Cloud - 1 Year (Monthly) Flowserve

This service leverages the Metallic Air Gap Protect offering from Commvault Cloud https://metallic.io/ to provide the long term retention storage target for Azure virtual machine backups.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Air Gap Protect for Service Providers, APJ, Azure Cool Tier (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611340 Air Gap Protect Azure Hot Storage APJ Data Protection by Commvault Cloud - 1 Year (Monthly) Flowserve

This service leverages the Metallic Air Gap Protect offering from Commvault Cloud https://metallic.io/ to provide the long term retention storage target for Azure virtual machine backups.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Air Gap Protect for Service Providers, APJ, Azure Hot Tier (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents

- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611341 Air Gap Protect Azure Cool Storage USCAN Data Protection by Commvault Cloud - 1 Month (Monthly) Flowserve

This service leverages the Metallic Air Gap Protect offering from Commvault Cloud https://metallic.io/ to provide the long term retention storage target for Azure virtual machine backups.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Air Gap Protect for Service Providers, US & Canada, Azure Cool Tier (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault

Systems, Inc and may be subject to change as determined by Commvault.

- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611342 Air Gap Protect Azure Hot Storage USCAN Data Protection by Commvault Cloud - 1 Month (Monthly) Flowserve

This service leverages the Metallic Air Gap Protect offering from Commvault Cloud https://metallic.io/ to provide the long term retention storage target for Azure virtual machine backups

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Air Gap Protect for Service Providers, US & Canada, Azure Hot Tier (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611343 Air Gap Protect Azure Cool Storage EMEA Data Protection by Commvault Cloud - 1 Month (Monthly) Flowserve

This service leverages the Metallic Air Gap Protect offering from Commvault Cloud https://metallic.io/ to provide the long-term retention storage target for Azure virtual machine backups.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Air Gap Protect for Service Providers, EMEA, Azure Cool Tier (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal

- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611344 Air Gap Protect Azure Hot Storage EMEA Data Protection by Commvault Cloud - 1 Month (Monthly) Flowserve

This service leverages the Metallic Air Gap Protect offering from Commvault Cloud https://metallic.io/ to provide the long-term retention storage target for Azure virtual machine backups.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Air Gap Protect for Service Providers, EMEA, Azure Hot Tier (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request

support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611345 Air Gap Protect Azure Cool Storage APJ Data Protection by Commvault Cloud - 1 Month (Monthly) Flowserve

This service leverages the Metallic Air Gap Protect offering from Commvault Cloud https://metallic.io/ to provide the long term retention storage target for Azure virtual machine backups.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Air Gap Protect for Service Providers, APJ, Azure Cool Tier (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at

https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611346 Air Gap Protect Azure Hot Storage APJ Data Protection by Commvault Cloud - 1 Month (Monthly) Flowserve

This service leverages the Metallic Air Gap Protect offering from Commvault Cloud https://metallic.io/ to provide the long term retention storage target for Azure virtual machine backups.

This is a client self-service offering supported by OneNeck.

Company's Responsibilities and Included Features

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The size of the stored data is measured as the largest peak size in gigabytes (GB) during the month stored. Data stored

equals the final amount of data stored on disk after de-duplication and compression algorithms have been applied. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Air Gap Protect for Service Providers, APJ, Azure Hot Tier (Commvault Offering). Client agrees`, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611347 File & Object Data Protection by Commvault Cloud - 1 Month (Monthly) Flowserve

This service leverages the Metallic offering from Commvault Cloud https://metallic.io/ to protect large file services on virtual machines, Azure Files and Azure blob storage.

Storage is included with this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The amount of storage protected is determined by the largest peak size in gigabytes (GB) protected GB of storage that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB Protected or front-end TB (FET).

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Backup & Recovery for Files & Objects for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611348 Database PaaS Data Protection by Commvault Cloud (Cloud Native and Enterprise) - 1 Month (Monthly) Flowserve

This service leverages the Metallic offering from Commvault Cloud https://metallic.io/ to protect supported cloud native (PaaS) and enterprise database applications.

Storage is included in this service.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
    - Policy definition
    - Backup job scheduling
    - Backup initiation
    - Restoration initiation
    - Data protection definition

        - Monitor backups and restores
        - Consumption reporting
    - Provide support, setup and configuration of backup policies (as requested by Client)
    - Provide support for initiation of backups and restorations (as requested by Client)
    - Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Microsoft Online Services level troubleshooting
    - Escalation to software provider
- To resolve system incidents, Company will:
    - Apply Company known solutions
    - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The amount of storage protected is determined by the largest peak size in gigabytes (GB) protected GB of storage that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB Protected or front-end TB (FET).

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Backup & Recovery for Databases for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611349 Active Directory Data Protection by Commvault Cloud (Active Directory, Azure Active Directory) - 1 Month (Monthly) Flowserve

This service leverages the Metallic offering from Commvault Cloud https://metallic.io/ to protect active directory data for enrolled users using a Company-provided backup software agent. Agent allows for backup and data protection and supports Active Directory and Azure Active Directory.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.

- The number of licenses is determined by the number unique clients of this type (User based) that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Backup & Recovery for Active Directory for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611350 VM & Kubernetes Data Protection by Commvault Cloud - 1 Month (Monthly) Flowserve

This service leverages the Metallic offering from Commvault Cloud https://metallic.io/ to protect virtual machine & Kubernetes data for enrolled VMs using a Company-provided backup software agent. Agent allows for backup and data protection down to the file level and supports backup of Microsoft SQL and Oracle database applications running on the virtual machine. Oracle RAC and SAP IaaS database applications running the virtual machine are also supported.

This service requires the use of the Metallic Air Gap Protect Azure Hot Storage and Metallic Air Gap Protect Azure Cool Storage.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number unique clients of this type (VM based) that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is per VM.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Backup & Recovery for VM for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611510 Active Directory Data Protection by Commvault Cloud (Active Directory, Azure Active Directory) - 1 Month (Monthly)

This service leverages the Metallic offering from Commvault Cloud https://metallic.io/ to protect active directory data for enrolled users using a Company-provided backup software agent. Agent allows for backup and data protection and supports Active Directory and Azure Active Directory.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
    - Policy definition
    - Backup job scheduling
    - Backup initiation
    - Restoration initiation

        - Data protection definition
        - Monitor backups and restores
        - Consumption reporting
    - Provide support, setup and configuration of backup policies (as requested by Client)
    - Provide support for initiation of backups and restorations (as requested by Client)
    - Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Microsoft Online Services level troubleshooting
    - Escalation to software provider
- To resolve system incidents, Company will:
    - Apply Company known solutions
    - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number unique clients of this type (User based) that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Backup & Recovery for Active Directory for Service Providers licensing of software (Commvault Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

611721 Commvault Cloud Clean Room Recovery SaaS - 1 Year (Monthly)

This service leverages the Commvault Cloud offering from Commvault Cloud https://metallic.io/ to provide a clean, secure, isolated recovery environment on demand for testing cyber recovery plans and conducting secure forensic analysis.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number unique clients of this type (User based) that are active within a

month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Clean Room Recovery SaaS for Service Providers licensing of software ("Commvault Offering"). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault's Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault's Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

This service leverages the Commvault Cloud offering from Commvault Cloud https://metallic.io/ to protect active directory data for enrolled users using a Company-provided backup software agent. Agent allows for backup and data protection and supports Active Directory and Azure Active Directory.

Company provides support for this self-service offering.

Company's Responsibilities and Included Features

Backup service details

- Provide Client access to an on-line self-service portal for the purpose of performing the following tasks:
  - Policy definition
  - Backup job scheduling
  - Backup initiation
  - Restoration initiation
  - Data protection definition
  - Monitor backups and restores
  - Consumption reporting
- Provide support, setup and configuration of backup policies (as requested by Client)
- Provide support for initiation of backups and restorations (as requested by Client)
- Provide self-service portal documentation

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for backup errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Microsoft Online Services level troubleshooting
  - Escalation to software provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply backup software vendor provided solutions
- Document user issues and system errors

Service Metering

- This service is delivered as a metered service allowing Client to consume managed software licensing.
- The number of licenses is determined by the number unique clients of this type (User based) that are active within a month. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is per User.

Terms

- This ItemID contains an order for Commvault Systems, Inc Commvault Cloud Backup & Recovery SaaS for Active Directory Enterprise for Service Providers licensing of software (“Commvault Offering”). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Commvault Offering will be provided and made by Commvault Systems, Inc and may be subject to change as determined by Commvault.
- Client agrees that the Commvault Offerings are subject to the then current Commvault Master Terms & Conditions available at https://www.commvault.com/legal/master-terms-and-conditions, Commvault’s Data Privacy Agreement located at https://metallic.io/commvault-data-agreement, and Commvault’s Security Terms located at https://metallic.io/security-terms, which are hereby incorporated into this Statement of Work.
- Company may revise terms of use or pricing to reflect changes by Commvault.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

-
  - 24 x 7 technical support for priority 1 and 2 incidents

- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This is a self-service offering.

Configuration and Setup

- Perform setup and configuration of backup services using the self-service portal.

Backup Operation

- Perform backup operation using the self-service portal
- Define backup content
- Define frequency, schedule, and retention of the backups
- Conduct Microsoft Online Services administration of users and resources subject to backup
- Validate data restored

Restore Operations

- Perform restore operations using the self-service portal
- Specify restore requirements including content, version, and restore target

Managed Backups

- Manage backup operations

Access

- Provide Company access to Microsoft Online Services and Azure Resources

810089 NB-MET Managed Metered Backup Service

Company's Responsibilities and Included Features

Item ID Description

NB-MET Managed Metered Backup Service

Company Responsibilities and Included Features

Backup Infrastructure

Company s centralized backup system is comprised of the following elements:

Client backup agents installed on each server

Centralized disk storage for disk to disk backups to reduce impact to server by minimizing backup duration

Additional de-duplicated disk storage devices for local backups for quick and easy restoration of recent backups

Large tape library with multiple drives, for creation of offsite tape backups and archive tapes

Multiple backup media servers

Backup management system for centralized management of backup media servers and backup policies

Backup infrastructure monitoring systems

Backup reporting systems

Tape Media and Off-site Tape Storage:
All tape media is provided for single copies of backups
Tape media for 35 day daily/weekly rotation cycle, monthly and yearly archiving is included
Off-site tape storage is provided through a leading off-site tape storage service provider providing daily off-site tape pickup
Client specific tapes are created.

Infrastructure Management:
Company maintains ongoing software support contracts for all hardware and software involved in the Centralized Backup infrastructure
Periodic upgrade of hardware and software is conducted to maintain support compliance and to provide new backup capabilities
Backup infrastructure, disks, tapes are all stored in Company s secure facility or off-site storage partner facility with proper chain of custody tracking of all Client proprietary assets

Backup Process
Backups are processed from the Client s hosted environments to Company s independent backup SAN infrastructure
Backups are then spooled to a data de-duplicated storage array for short term local backups (limited to up to 35 days)
Backups are copied to tape from the backup SAN infrastructure and then rotated off-site daily
Backup alerts and reports are provided to Company server, database and application administrators for analysis and corrective action
Company applies commercially reasonable effort to conduct timely backups of all Client proprietary data as defined in the backup policies
Daily and weekly tapes are rotated on a 35 day cycle. Customized retention/rotation cycles are available for an additional charge.

Backup Metering
This is a metered service.
Metering is based upon the total volume in GB of data transferred to the Centralized Backup system over the billing period.

Backup Schedules
Backup schedules are defined by the Client.
Standard or Best practice schedules typically applied are as follows:
Production Databases
Backup Type Scheduled Frequency
Full Backup Once Per Week
Incremental Backup Every day unless a Full Backup is scheduled
Transaction Backups Every 4 hours Around the clock

Test/Development Databases
Backup Type Scheduled Frequency
Full Backup Once Every Other Week
Incremental Backup Every week unless a Full Backup is scheduled
Transaction Backups Every 12 hours Around the clock

Archive Databases
Backup Type Scheduled Frequency
Full Backup (Monthly) Once a Month with 13 Month Retention unless archiving activity is anticipated.
Incremental Backup None
Transaction Backups Every week a Full Backup is NOT Scheduled

File System Backups
Backup Type Scheduled Frequency
Full Backup Once Per Week
Incremental Backup Daily

This process ensures that:
Production databases can be recovered to almost any point in time going back 28 days with a maximum potential for data loss of 4 hours in the event of a source hardware failure.
File Systems can be recovered going back daily for 35 days with a maximum potential for data loss of 24 hours in the event of a source hardware failure

Backup Agents
Backup agents are required on each server being backed up
Multiple backup agents may be required for each server depending on what is being backed up (File system, database, email)
Company provides the backup agents.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)
Client's Responsibilities and Out-of-Scope Notes (unless otherwise covered via a different Item ID)
Backup Policy Definition
Client is responsible for defining:
What must be backed up
When and how often it must be backed up
How it must be backed up. (Full, Incremental, Differential)
Local backup retention policy
Archive tape content, timing and retention policy

Category: Cloud Integration

110049 Colocation Environment - Connection Service 10 Gbps

Company's Responsibilities and Included Features

ReliaCloud Colocation Integration services delivers 10 GBps layer 3 connectivity services to colocated cabinet(s) environment. The service requires at least two physical connections to provide path and infrastructure diversity such the ReliaCloud standard SLA can be delivered. The service is designed to offer an extension of infrastructure services from ReliaCloud to Colocation cabinet. The connection is layer 3 based to prevent conflicts with switching convergence.

- Provide managed LAN services which provides speeds up to 10 GBps
- Provide all physical cabling to interconnect the hosted device to the ReliaCloud switching infrastructure
- Deliver services over Cat6 or greater RJ-45 Ethernet
- Design, manage and maintain VLAN configuration
- Maintain ACLs
- Notify Client of any performance challenges or link-state issues with the service
- Provide monitoring statics on port speed and performance

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide physical device for termination of service
- Ensure device supports at least 2 1 GBps RJ-45 Ethernet interfaces

601507

Company's Responsibilities and Included Features

The ReliaCloud EXTEND 250W Device Integration Service, provides secured space for a single device or chassis (Device) with up to 250 watts of typical power consumption/steady-state power draw as rated by the Device manufacturer. The service is designed to allow a Client Device to integrate with ReliaCloud Services. Company will provide the following services:

- Provide a secure four-sided locking cabinet to host the Device. Cabinets are multi-tenant and under the exclusive control of Company
- Provide continuous power to the Device via A and B side power feeds
    - If more than one A-side and one B-side cord is needed per-Device, Company will use split cords
    - Power receptacles may plug-in directly behind a Device's power supply, requiring a planned power-down of the Device in order to replace a power supply/fan in the Device
- Ensure proper power load distribution across A and B power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all physical moves, adds, and changes for the device per ticket request

Restrictions

- Device must be approved by Company
- Service only supports 208v Devices
- Service limited to 250W of steady state power (maximum power allocation)
- Device power plug type must be compatible with C-13 or C-19 outlets
- Device must contain A and B side power capability. Devices containing less than two (2) power supplies will void any applicable service level agreement herein and therefore are ineligible for service credits.
- Device must be rack-mountable within 4-post locking cabinet, using front-side mounting only (maximum protrusion one (1) inch
- Device must exhaust heat to back of the cabinet

- No physical access is granted to Client to the Device while installed
- Units of service cannot be combined to support a single larger Device
- If a Device exceeds the maximum power allocation more than three times in any calendar month, Client will execute a change order for the next higher power rating ReliaCloud EXTEND Device Integration Service

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide Company with means to access any physically secured Devices (i.e. keys to faceplate locks)
- Contract ReliaCloud Extend Device Network Connection Service
- Provide Device power cables
- Device must be contracted for the steady state power of the maximum configuration. For example, if a device starts out with 250 watts of steady state power, though it is scalable to 1000 watts of steady state power through the physical addition of nodes, that device must contract for 1000 watts of service.

601508

Company's Responsibilities and Included Features

The ReliaCloud EXTEND 500W Device Integration Service, provides secured space for a single device or chassis (Device) with up to 500 watts of typical power consumption/steady-state power draw as rated by the Device manufacturer. The service is designed to allow a Client Device to integrate with ReliaCloud Services. Company will provide the following services:

- Provide a secure four-sided locking cabinet to host the Device. Cabinets are multi-tenant and under the exclusive control of Company
- Provide continuous power to the Device via A and B side power feeds
    - If more than one A-side and one B-side cord is needed per-Device, Company will use split cords
    - Power receptacles may plug-in directly behind a Device's power supply, requiring a planned power-down of the Device in order to replace a power supply/fan in the Device
- Ensure proper power load distribution across A and B power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all physical moves, adds, and changes for the device per ticket request

Restrictions

- Device must be approved by Company
- Service only supports 208v Devices
- Service limited to 500W of steady state power (maximum power allocation)
- Device power plug type must be compatible with C-13 or C-19 outlets
- Device must contain A and B side power capability. Devices containing less than two (2) power supplies will void any applicable service level agreement herein and therefore are ineligible for service credits.
- Device must be rack-mountable within 4-post locking cabinet, using front-side mounting only (maximum protrusion one (1) inch
- Device must exhaust heat to back of the cabinet
- No physical access is granted to Client to the Device while installed
- Units of service cannot be combined to support a single larger Device
- If a Device exceeds the maximum power allocation more than three times in any calendar month, Client will execute a change order for the next higher power rating ReliaCloud EXTEND Device Integration Service

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide Company with means to access any physically secured Devices (i.e. keys to faceplate locks)

Contract ReliaCloud Extend Device Network Connection Service
- Provide Device power cables
- Device must be contracted for the steady state power of the maximum configuration. For example, if a device starts out with 250 watts of steady state power, though it is scalable to 1000 watts of steady state power through the physical addition of nodes, that device must contract for 1000 watts of service.

601509

Company's Responsibilities and Included Features

The ReliaCloud EXTEND 750W Device Integration Service, provides secured space for a single device or chassis (Device) with up to 750 watts of typical power consumption/steady-state power draw as rated by the Device manufacturer. The service is designed to allow a Client Device to integrate with ReliaCloud Services. Company will provide the following services:

- Provide a secure four-sided locking cabinet to host the Device. Cabinets are multi-tenant and under the exclusive control of Company
- Provide continuous power to the Device via A and B side power feeds
  - If more than one A-side and one B-side cord is needed per-Device, Company will use split cords
  - Power receptacles may plug-in directly behind a Device's power supply, requiring a planned power-down of the Device in order to replace a power supply/fan in the Device
- Ensure proper power load distribution across A and B power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all physical moves, adds, and changes for the device per ticket request

Restrictions

- Device must be approved by Company
- Service only supports 208v Devices
- Service limited to 750W of steady state power (maximum power allocation)
- Device power plug type must be compatible with C-13 or C-19 outlets
- Device must contain A and B side power capability. Devices containing less than two (2) power supplies will void any applicable service level agreement herein and therefore are ineligible for service credits.
- Device must be rack-mountable within 4-post locking cabinet, using front-side mounting only (maximum protrusion one (1) inch
- Device must exhaust heat to back of the cabinet
- No physical access is granted to Client to the Device while installed
- Units of service cannot be combined to support a single larger Device
- If a Device exceeds the maximum power allocation more than three times in any calendar month, Client will execute a change order for the next higher power rating ReliaCloud EXTEND Device Integration Service

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide Company with means to access any physically secured Devices (i.e. keys to faceplate locks)
- Contract ReliaCloud Extend Device Network Connection Service
- Provide Device power cables
- Device must be contracted for the steady state power of the maximum configuration. For example, if a device starts out with 250 watts of steady state power, though it is scalable to 1000 watts of steady state power through the physical addition of nodes, that device must contract for 1000 watts of service.

601510

Company's Responsibilities and Included Features

The ReliaCloud EXTEND 1000W Device Integration Service, provides secured space for a single device or chassis (Device) with

up to 1000 watts of typical power consumption/steady-state power draw as rated by the Device manufacturer. The service is designed to allow a Client Device to integrate with ReliaCloud Services. Company will provide the following services:

- Provide a secure four-sided locking cabinet to host the Device. Cabinets are multi-tenant and under the exclusive control of Company
- Provide continuous power to the Device via A and B side power feeds
    - If more than one A-side and one B-side cord is needed per-Device, Company will use split cords
    - Power receptacles may plug-in directly behind a Device's power supply, requiring a planned power-down of the Device in order to replace a power supply/fan in the Device
- Ensure proper power load distribution across A and B power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all physical moves, adds, and changes for the device per ticket request

Restrictions

- Device must be approved by Company
- Service only supports 208v Devices
- Service limited to 1000W of steady state power (maximum power allocation)
- Device power plug type must be compatible with C-13 or C-19 outlets
- Device must contain A and B side power capability. Devices containing less than two (2) power supplies will void any applicable service level agreement herein and therefore are ineligible for service credits.
- Device must be rack-mountable within 4-post locking cabinet, using front-side mounting only (maximum protrusion one (1) inch
- Device must exhaust heat to back of the cabinet
- No physical access is granted to Client to the Device while installed
- Units of service cannot be combined to support a single larger Device
- If a Device exceeds the maximum power allocation more than three times in any calendar month, Client will execute a change order for the next higher power rating ReliaCloud EXTEND Device Integration Service

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide Company with means to access any physically secured Devices (i.e. keys to faceplate locks)
- Contract ReliaCloud Extend Device Network Connection Service
- Provide Device power cables
- Device must be contracted for the steady state power of the maximum configuration. For example, if a device starts out with 250 watts of steady state power, though it is scalable to 1000 watts of steady state power through the physical addition of nodes, that device must contract for 1000 watts of service.

601511

Company's Responsibilities and Included Features

The ReliaCloud EXTEND 2000W Device Integration Service, provides secured space for a single device or chassis (Device) with up to 2000 watts of typical power consumption/steady-state power draw as rated by the Device manufacturer. The service is designed to allow a Client Device to integrate with ReliaCloud Services. Company will provide the following services:

- Provide a secure four-sided locking cabinet to host the Device. Cabinets are multi-tenant and under the exclusive control of Company
- Provide continuous power to the Device via A and B side power feeds
    - If more than one A-side and one B-side cord is needed per-Device, Company will use split cords
    - Power receptacles may plug-in directly behind a Device's power supply, requiring a planned power-down of the Device in order to replace a power supply/fan in the Device
- Ensure proper power load distribution across A and B power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet

Provide all physical moves, adds, and changes for the device per ticket request

Restrictions

- Device must be approved by Company
- Service only supports 208v Devices
- Service limited to 2000W of steady state power (maximum power allocation)
- Device power plug type must be compatible with C-13 or C-19 outlets
- Device must contain A and B side power capability. Devices containing less than two (2) power supplies will void any applicable service level agreement herein and therefore are ineligible for service credits.
- Device must be rack-mountable within 4-post locking cabinet, using front-side mounting only (maximum protrusion one (1) inch
- Device must exhaust heat to back of the cabinet
- No physical access is granted to Client to the Device while installed
- Units of service cannot be combined to support a single larger Device
- If a Device exceeds the maximum power allocation more than three times in any calendar month, Client will execute a change order for the next higher power rating ReliaCloud EXTEND Device Integration Service

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide Company with means to access any physically secured Devices (i.e. keys to faceplate locks)
- Contract ReliaCloud Extend Device Network Connection Service
- Provide Device power cables
- Device must be contracted for the steady state power of the maximum configuration. For example, if a device starts out with 250 watts of steady state power, though it is scalable to 1000 watts of steady state power through the physical addition of nodes, that device must contract for 1000 watts of service.

601512

Company's Responsibilities and Included Features

The ReliaCloud EXTEND Network Connection Service provides the ability for Client-provided device or chassis (Device) to connect into ReliaCloud at up to 25 Gbps port speed. Company will provide the following services:

- Provide a network connection that supports up to 25 Gbps port speed
- Provide cables between Company equipment and Device
- Provide small form-factor pluggable transceivers (SFP s) for Company s side of the connection
- Service is Layer 2
- VLAN configuration activities, including provisions of secure VLAN trunks
- Service is a single network connection and requires two (2) network connections to provide a highly available solution
- Upon Client request, service supports port-channel / link-aggregation configuration using Link Aggregation Control Protocol (LACP) or static configuration
- Service supports the following connections:
    - 25GBASE-SR (25G over Multimode Fiber)
    - 25GBASE-LR (25G over Singlemode Fiber)
    - 25GBASE-CR (25G DAC) Company-managed Nutanix devices onlyevice must be approved by Company

Restrictions

- Client-provided SFPs must be approved by Company
- Service does not support spanning-tree bridge protocol data units (BPDU); Company will automatically disable the port if BPDUs are detected
- Storm control will be used to suppress unusually high rates of broadcast, multicast, and/or unknown unicast packets
- Service speeds are fixed once delivered. Change speeds requires changing optics and physical ports and services

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide SFPs for Client s side of the connection
- Contract for two (2) quantities of the Service for highly available services per attached Device. Client s failure to do so will void any applicable service level agreement herein and Client will be ineligible for associated service credits
- When connecting a physical device, ensure Device supports at least two (2) 25 Gbps connections and has appropriate cards/modules that facilitate the connection
- Configuration of attached Device for teaming or multipathing

601513

Company's Responsibilities and Included Features

The ReliaCloud EXTEND Network Connection Service provides the ability for Client-provided device or chassis (Device) to connect into ReliaCloud at up to 10 Gbps port speed. Company will provide the following services:

- Provide a network connection that supports up to 10 Gbps port speed
- Provide cables between Company equipment and Device
- Provide small form-factor pluggable transceivers (SFP s) for Company s side of the connection
- Service is Layer 2
- VLAN configuration activities, including provisions of secure VLAN trunks
- Service is a single network connection and requires two (2) network connections to provide a highly available solution
- Upon Client request, service supports port-channel / link-aggregation configuration using Link Aggregation Control Protocol (LACP) or static configuration
- Service supports the following connections:
    - 10GBASE-SR (10G over Multimode Fiber)
    - 10GBASE-LR (10G over Singlemode Fiber)
    - 10GBASE-CR (10G DAC) Company-managed Nutanix devices only. Device must be approved by Company

Restrictions

- Client-provided SFPs must be approved by Company
- Service does not support spanning-tree bridge protocol data units (BPDU); Company will automatically disable the port if BPDUs are detected
- Storm control will be used to suppress unusually high rates of broadcast, multicast, and/or unknown unicast packets
- Service speeds are fixed once delivered. Change speeds requires changing optics and physical ports and services

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide SFPs for Client s side of the connection
- Contract for two (2) quantities of the Service for highly available services per attached Device. Client s failure to do so will void any applicable service level agreement herein and Client will be ineligible for associated service credits
- When connecting a physical device, ensure Device supports at least two (2) 10 Gbps connections and has appropriate cards/modules that facilitate the connection
- Configuration of attached Device for teaming or multipathing

601514

Company's Responsibilities and Included Features

The ReliaCloud EXTEND Network Connection Service provides the ability for Client-provided device or chassis (Device) to connect into ReliaCloud at up to 1 Gbps port speed. Company will provide the following services:

- Provide a network connection that supports up to 1 Gbps port speed
- Provide cables between Company equipment and Device
- Provide small form-factor pluggable transceivers (SFP s) for Company s side of the connection

Service is Layer 2
- VLAN configuration activities, including provisions of secure VLAN trunks
- Service is a single network connection and requires two (2) network connections to provide a highly available solution
- Upon Client request, service supports port-channel / link-aggregation configuration using Link Aggregation Control Protocol (LACP) or static configuration
- Service delivered over 1000BASE-T

Restrictions

- Client-provided SFPs must be approved by Company
- Service does not support spanning-tree bridge protocol data units (BPDU); Company will automatically disable the port if BPDUs are detected
- Storm control will be used to suppress unusually high rates of broadcast, multicast, and/or unknown unicast packets
- Service speeds are fixed once delivered. Change speeds requires changing optics and physical ports and services

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide SFPs for Client s side of the connection
- Contract for two (2) quantities of the Service for highly available services per attached Device. Client s failure to do so will void any applicable service level agreement herein and Client will be ineligible for associated service credits
- When connecting a physical device, ensure Device supports at least two (2) 1 Gbps connections and has appropriate cards/modules that facilitate the connection
- Configuration of attached Device for teaming or multipathing

601515

Company's Responsibilities and Included Features

The ReliaCloud EXTEND Out-of-Band Management Connection provides a low-speed (up to 1 Gbps) network connection for the purpose of connecting to a Client device that is equipped with an out-of-band or lights-out management interface. Company will provide the following services:

- Provide a low-speed management class network connection that supports up to one (1) Gbps port speed
- Provide cable between Company equipment and Client device
- Service is Layer 2
- Service is a single (1) network connection per device
- Service supports 1000BASE-T over CAT5e or greater connections

Restrictions

- Device is not designed to service a primary network connection
- Service does not support spanning-tree bridge protocol data unit (BPDU). Company will automatically disable the port if BPDUs are detected
- Storm control will be used to suppress unusually high rates of broadcast, multicast, and/or unknown unicast packets

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide small form-factor pluggable transceivers (SFP) for Client side of the connection if required (typically not required)

601683 ReliaCloud EXTEND - 100W Device Integration Service

Company's Responsibilities and Included Features

The ReliaCloud EXTEND 100W Device Integration Service, provides secured space for a single device or chassis (Device) with up to 100 watts of typical power consumption/steady-state power draw as rated by the Device manufacturer. The service is designed to allow a Client Device to integrate with ReliaCloud Services. Company will provide the following services:

- Provide a secure four-sided locking cabinet to host the Device. Cabinets are multi-tenant and under the exclusive control of Company
- Provide continuous power to the Device via A and B side power feeds
    - If more than one A-side and one B-side cord is needed per-Device, Company will use split cords
    - Power receptacles may plug-in directly behind a Device's power supply, requiring a planned power-down of the Device in order to replace a power supply/fan in the Device
- Ensure proper power load distribution across A and B power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all physical moves, adds, and changes for the device per ticket request

Restrictions

- Device must be approved by Company
- Service only supports 208v Devices
- Service limited to 100W of steady state power (maximum power allocation)
- Device power plug type must be compatible with C-13 or C-19 outlets
- Device must contain A and B side power capability. Devices containing less than two (2) power supplies will void any applicable service level agreement herein and therefore are ineligible for service credits.
- Device must be rack-mountable within 4-post locking cabinet, using front-side mounting only (maximum protrusion one (1) inch
- Device must exhaust heat to back of the cabinet
- No physical access is granted to Client to the Device while installed
- Units of service cannot be combined to support a single larger Device
- If a Device exceeds the maximum power allocation more than three times in any calendar month, Client will execute a change order for the next higher power rating ReliaCloud EXTEND Device Integration Service

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide Company with means to access any physically secured Devices (i.e. keys to faceplate locks)
- Contract ReliaCloud Extend Device Network Connection Service
- Provide Device power cables
- Device must be contracted for the steady state power of the maximum configuration. For example, if a device starts out with 250 watts of steady state power, though it is scalable to 1000 watts of steady state power through the physical addition of nodes, that device must contract for 1000 watts of service.

604180 ReliaCloud EXTEND - 500W Device Integration Service

Company's Responsibilities and Included Features

The ReliaCloud EXTEND 500W Device Integration Service, provides secured space for a single device or chassis (Device) with up to 500 watts of typical power consumption/steady-state power draw as rated by the Device manufacturer. The service is designed to allow a Client Device to integrate with ReliaCloud Services. Company will provide the following services:

- Provide a secure four-sided locking cabinet to host the Device. Cabinets are multi-tenant and under the exclusive control of Company
- Provide continuous power to the Device via A and B side power feeds
    - If more than one A-side and one B-side cord is needed per-Device, Company will use split cords
    - Power receptacles may plug-in directly behind a Device's power supply, requiring a planned power-down of the Device in order to replace a power supply/fan in the Device
- Ensure proper power load distribution across A and B power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet

- Provide all physical moves, adds, and changes for the device per ticket request

Restrictions

- Device must be approved by Company
- Service only supports 208v Devices
- Service limited to 500W of steady state power (maximum power allocation)
- Device power plug type must be compatible with C-13 or C-19 outlets
- Device must contain A and B side power capability. Devices containing less than two (2) power supplies will void any applicable service level agreement herein and therefore are ineligible for service credits.
- Device must be rack-mountable within 4-post locking cabinet, using front-side mounting only (maximum protrusion one (1) inch
- Device must exhaust heat to back of the cabinet
- No physical access is granted to Client to the Device while installed
- Units of service cannot be combined to support a single larger Device
- If a Device exceeds the maximum power allocation more than three times in any calendar month, Client will execute a change order for the next higher power rating ReliaCloud EXTEND Device Integration Service

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide Company with means to access any physically secured Devices (i.e. keys to faceplate locks)
- Contract ReliaCloud Extend Device Network Connection Service
- Provide Device power cables
- Device must be contracted for the steady state power of the maximum configuration. For example, if a device starts out with 250 watts of steady state power, though it is scalable to 1000 watts of steady state power through the physical addition of nodes, that device must contract for 1000 watts of service.

604181 ReliaCloud EXTEND - 10 Gbps Network Connection Service

Company's Responsibilities and Included Features

The ReliaCloud EXTEND Network Connection Service provides the ability for Client-provided device or chassis (Device) to connect into ReliaCloud at up to 10 Gbps port speed. Company will provide the following services:

- Provide a network connection that supports up to 10 Gbps port speed
- Provide cables between Company equipment and Device
- Provide small form-factor pluggable transceivers (SFP s) for Company s side of the connection
- Service is Layer 2
- VLAN configuration activities, including provisions of secure VLAN trunks
- Service is a single network connection and requires two (2) network connections to provide a highly available solution
- Upon Client request, service supports port-channel / link-aggregation configuration using Link Aggregation Control Protocol (LACP) or static configuration
- Service supports the following connections:
    - 10GBASE-SR (10G over Multimode Fiber)
    - 10GBASE-LR (10G over Singlemode Fiber)
    - 10GBASE-CR (10G DAC) Company-managed Nutanix devices only. Device must be approved by Company

Restrictions

- Client-provided SFPs must be approved by Company
- Service does not support spanning-tree bridge protocol data units (BPDU); Company will automatically disable the port if BPDUs are detected
- Storm control will be used to suppress unusually high rates of broadcast, multicast, and/or unknown unicast packets
- Service speeds are fixed once delivered. Change speeds requires changing optics and physical ports and services

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide SFPs for Client s side of the connection
- Contract for two (2) quantities of the Service for highly available services per attached Device. Client s failure to do so will void any applicable service level agreement herein and Client will be ineligible for associated service credits
- When connecting a physical device, ensure Device supports at least two (2) 10 Gbps connections and has appropriate cards/modules that facilitate the connection
- Configuration of attached Device for teaming or multipathing

604182 ReliaCloud EXTEND - Out-of-Band Management Connection

Company's Responsibilities and Included Features

The ReliaCloud EXTEND Out-of-Band Management Connection provides a low-speed (up to 1 Gbps) network connection for the purpose of connecting to a Client device that is equipped with an out-of-band or lights-out management interface. Company will provide the following services:

- Provide a low-speed management class network connection that supports up to one (1) Gbps port speed
- Provide cable between Company equipment and Client device
- Service is Layer 2
- Service is a single (1) network connection per device
- Service supports 1000BASE-T over CAT5e or greater connections

Restrictions

- Device is not designed to service a primary network connection
- Service does not support spanning-tree bridge protocol data unit (BPDU). Company will automatically disable the port if BPDUs are detected
- Storm control will be used to suppress unusually high rates of broadcast, multicast, and/or unknown unicast packets

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide small form-factor pluggable transceivers (SFP) for Client side of the connection if required (typically not required)

604183 ReliaCloud EXTEND - 1 Gbps Network Connection Service

Company's Responsibilities and Included Features

The ReliaCloud EXTEND Network Connection Service provides the ability for Client-provided device or chassis (Device) to connect into ReliaCloud at up to 1 Gbps port speed. Company will provide the following services:

- Provide a network connection that supports up to 1 Gbps port speed
- Provide cables between Company equipment and Device
- Provide small form-factor pluggable transceivers (SFP s) for Company s side of the connection
- Service is Layer 2
- VLAN configuration activities, including provisions of secure VLAN trunks
- Service is a single network connection and requires two (2) network connections to provide a highly available solution
- Upon Client request, service supports port-channel / link-aggregation configuration using Link Aggregation Control Protocol (LACP) or static configuration
- Service delivered over 1000BASE-T

Restrictions

- Client-provided SFPs must be approved by Company
- Service does not support spanning-tree bridge protocol data units (BPDU); Company will automatically disable the port if BPDUs are detected

- Storm control will be used to suppress unusually high rates of broadcast, multicast, and/or unknown unicast packets
- Service speeds are fixed once delivered. Change speeds requires changing optics and physical ports and services

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide SFPs for Client s side of the connection
- Contract for two (2) quantities of the Service for highly available services per attached Device. Client s failure to do so will void any applicable service level agreement herein and Client will be ineligible for associated service credits
- When connecting a physical device, ensure Device supports at least two (2) 1 Gbps connections and has appropriate cards/modules that facilitate the connection
- Configuration of attached Device for teaming or multipathing

Category: Cloud Transport

500206 OneNeck Connect for Data Centers - Layer 3 - 10Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocation environments or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 10 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection to any ReliaCloud workload.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least two instances of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 3 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500207 OneNeck Connect for Data Centers - Layer 3 - 25Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocation environments or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 25 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection to any ReliaCloud workload.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least two instances of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 3 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500208 OneNeck Connect for Data Centers - Layer 3 - 50Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocation environments or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 50 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection to any ReliaCloud workload.

- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least two instances of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 3 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500209 OneNeck Connect for Data Centers - Layer 3 - 100Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocation environments or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 100 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection to any ReliaCloud workload.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least two instances of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 3 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500210 OneNeck Connect for Data Centers - Layer 3 - 200Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocation environments or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 200 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection to any ReliaCloud workload.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least two instances of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 3 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500211 OneNeck Connect for Data Centers - Layer 3 - 500Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocation environments or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 500 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.

- The service includes a cross-connection to any ReliaCloud workload.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least two instances of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 3 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500212 OneNeck Connect for Data Centers - Layer 3 - 1000Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocation environments or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 1000 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection to any ReliaCloud workload.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least two instances of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 3 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500213 OneNeck Connect for Data Centers - Layer 3 - 2000Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocation environments or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 2000 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection to any ReliaCloud workload.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least two instances of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 3 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500214 OneNeck Connect for Data Centers - Layer 3 - 3000Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocation environments or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 3000 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.

- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection to any ReliaCloud workload.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least two instances of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 3 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500215 OneNeck Connect for Data Centers - Layer 2 - 10Mbps

Company's Responsibilities and Included Features

Description:
The Layer-2 E-Line service provides an Ethernet circuit, interconnecting Company colocation environments, carriers in Company telecommunications rooms, and physical cross-connects to Company colocation environments or carrier hotels.

Service details:

- Managed transport services with a capped bandwidth of 10 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of this service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500216 OneNeck Connect for Data Centers - Layer 2 - 25Mbps

Company's Responsibilities and Included Features

Description:
The Layer-2 E-Line service provides an Ethernet circuit, interconnecting Company colocation environments, carriers in

Company telecommunications rooms, and physical cross-connects to Company colocation environments or carrier hotels.

Service details:

- Managed transport services with a capped bandwidth of 25 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of this service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500217 OneNeck Connect for Data Centers - Layer 2 - 50Mbps

Company's Responsibilities and Included Features

Description:
The Layer-2 E-Line service provides an Ethernet circuit, interconnecting Company colocation environments, carriers in Company telecommunications rooms, and physical cross-connects to Company colocation environments or carrier hotels.

Service details:

- Managed transport services with a capped bandwidth of 50 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of this service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.

For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500218 OneNeck Connect for Data Centers - Layer 2 - 100Mbps

Company's Responsibilities and Included Features

Description:
The Layer-2 E-Line service provides an Ethernet circuit, interconnecting Company colocation environments, carriers in Company telecommunications rooms, and physical cross-connects to Company colocation environments or carrier hotels.

Service details:

- Managed transport services with a capped bandwidth of 100 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of this service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500219 OneNeck Connect for Data Centers - Layer 2 - 200Mbps

Company's Responsibilities and Included Features

Description:
The Layer-2 E-Line service provides an Ethernet circuit, interconnecting Company colocation environments, carriers in Company telecommunications rooms, and physical cross-connects to Company colocation environments or carrier hotels.

Service details:

- Managed transport services with a capped bandwidth of 200 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.

- The service requires exactly two instances of this service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500220 OneNeck Connect for Data Centers - Layer 2 - 500Mbps

Company's Responsibilities and Included Features

Description:
The Layer-2 E-Line service provides an Ethernet circuit, interconnecting Company colocation environments, carriers in Company telecommunications rooms, and physical cross-connects to Company colocation environments or carrier hotels.

Service details:

- Managed transport services with a capped bandwidth of 500 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of this service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500221 OneNeck Connect for Data Centers - Layer 2 - 1000Mbps

Company's Responsibilities and Included Features

Description:
The Layer-2 E-Line service provides an Ethernet circuit, interconnecting Company colocation environments, carriers in Company telecommunications rooms, and physical cross-connects to Company colocation environments or carrier hotels.

Service details:

- Managed transport services with a capped bandwidth of 1000 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at each service location.

- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of this service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500224 OneNeck Connect for Data Centers (PHX2) - Layer 3 - 10Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting Client environments in Company Tempe data center to Company ReliaCloud and colocation environments, telecommunications MPLS clouds or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 10 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over non-redundant routes, with non-redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper).
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection in the Company Tempe data center.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service or carrier hotels extension as this service is only accounting for one side of a connection. Using this method, two or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500225 OneNeck Connect for Data Centers (PHX2) - Layer 3 - 25Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting Client environments in Company Tempe data center to Company ReliaCloud and colocation environments, telecommunications MPLS clouds or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 25 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over non-redundant routes, with non-redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper).
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection in the Company Tempe data center.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service or carrier hotels extension as this service is only accounting for one side of a connection. Using this method, two or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500226 OneNeck Connect for Data Centers (PHX2) - Layer 3 - 50Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting Client environments in Company Tempe data center to Company ReliaCloud and colocation environments, telecommunications MPLS clouds or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 50 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over non-redundant routes, with non-redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper).
- Service does not provide any encryption level services.

The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.

- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection in the Company Tempe data center.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service or carrier hotels extension as this service is only accounting for one side of a connection. Using this method, two or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500227 OneNeck Connect for Data Centers (PHX2) - Layer 3 - 100Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting Client environments in Company Tempe data center to Company ReliaCloud and colocation environments, telecommunications MPLS clouds or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 10 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over non-redundant routes, with non-redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper).
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection in the Company Tempe data center.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service or carrier hotels extension as this service is only accounting for one side of a connection. Using this method, two or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.

- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500228 OneNeck Connect for Data Centers (PHX2) - Layer 3 - 200Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting Client environments in Company Tempe data center to Company ReliaCloud and colocation environments, telecommunications MPLS clouds or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 200 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over non-redundant routes, with non-redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper).
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection in the Company Tempe data center.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service or carrier hotels extension as this service is only accounting for one side of a connection. Using this method, two or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500229 OneNeck Connect for Data Centers (PHX2) - Layer 3 - 500Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting Client environments in Company Tempe data center to Company ReliaCloud and colocation environments, telecommunications MPLS clouds or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 500 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over non-redundant routes, with non-redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper).

- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection in the Company Tempe data center.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service or carrier hotels extension as this service is only accounting for one side of a connection. Using this method, two or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500230 OneNeck Connect for Data Centers (PHX2) - Layer 3 - 1000Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting Client environments in Company Tempe data center to Company ReliaCloud and colocation environments, telecommunications MPLS clouds or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 1000 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over non-redundant routes, with non-redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper).
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection in the Company Tempe data center.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service or carrier hotels extension as this service is only accounting for one side of a connection. Using this method, two or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.

- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500231 OneNeck Connect for Data Centers (PHX2) - Layer 3 - 2000Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting Client environments in Company Tempe data center to Company ReliaCloud and colocation environments, telecommunications MPLS clouds or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 2000 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over non-redundant routes, with non-redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper).
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection in the Company Tempe data center.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service or carrier hotels extension as this service is only accounting for one side of a connection. Using this method, two or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500232 OneNeck Connect for Data Centers (PHX2) - Layer 3 - 3000Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting Client environments in Company Tempe data center to Company ReliaCloud and colocation environments, telecommunications MPLS clouds or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 3000 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over non-redundant routes, with non-redundant physical or virtual interconnects at each service location.

- Service delivery support on Cat5e (Copper).
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection in the Company Tempe data center.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service or carrier hotels extension as this service is only accounting for one side of a connection. Using this method, two or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

500233 OneNeck Connect for Data Centers with Azure Cross-connect - 50Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, connecting Azure environments to Company data centers.

Service details:

- Managed transport services with a committed bandwidth of 50 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 50 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service does not provide any encryption level services
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection to the Azure network.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 2 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- An Azure Express Route subscription.

500234 OneNeck Connect for Data Centers with Azure Cross-connect - 100Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, connecting Azure environments to Company data centers.

Service details:

- Managed transport services with a committed bandwidth of 100 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 50 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service does not provide any encryption level services
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection to the Azure network.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 2 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- An Azure Express Route subscription.

500235 OneNeck Connect for Data Centers with Azure Cross-connect - 200Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, connecting Azure environments to Company data centers.

Service details:

- Managed transport services with a committed bandwidth of 200 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 50 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service does not provide any encryption level services
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection to the Azure network.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 2 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- An Azure Express Route subscription.

500236 OneNeck Connect for Data Centers with Azure Cross-connect - 500Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, connecting Azure environments to Company data centers.

Service details:

- Managed transport services with a committed bandwidth of 500 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 50 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service does not provide any encryption level services
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection to the Azure network.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 2 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- An Azure Express Route subscription.

500237 OneNeck Connect for Data Centers with Azure Cross-connect - 1000Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, connecting Azure environments to Company data centers.

Service details:

- Managed transport services with a committed bandwidth of 1000 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 50 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service does not provide any encryption level services
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection to the Azure network.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 2 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- An Azure Express Route subscription.

500238 OneNeck Connect for Data Centers with Azure Cross-connect - 2000Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, connecting Azure environments to Company data centers.

Service details:

- Managed transport services with a committed bandwidth of 2000 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 50 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service does not provide any encryption level services
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection to the Azure network.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 2 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- An Azure Express Route subscription.

500239 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 3 - 10Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocations or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 10 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at the service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 2 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires an intra carrier hotel cross-connection for physical interconnect (colocation or carrier).

500240 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 3 - 25Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocations or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 25 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at the service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 2 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires an intra carrier hotel cross-connection for physical interconnect (colocation or carrier).

500241 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 3 - 50Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocations or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 50 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at the service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 2 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires an intra carrier hotel cross-connection for physical interconnect (colocation or carrier).

500242 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 3 - 100Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocations or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 100 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at the service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 2 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires an intra carrier hotel cross-connection for physical interconnect (colocation or carrier).

500243 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 3 - 200Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocations or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 200 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at the service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 2 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires an intra carrier hotel cross-connection for physical interconnect (colocation or carrier).

500244 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 3 - 500Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocations or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 500 Mbps.

- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at the service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 2 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires an intra carrier hotel cross-connection for physical interconnect (colocation or carrier).

500245 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 3 - 1000Mbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocations or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 1000 Mbps.
- The port or virtual port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at the service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 2 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.

- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires an intra carrier hotel cross-connection for physical interconnect (colocation or carrier).

500246 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 2 - 10Mbps

Company's Responsibilities and Included Features

Description:
The Layer-2 E-Line service provides an Ethernet circuit, interconnecting carrier hotel to Company colocation facilities.

Service details:

- Managed transport services with a capped bandwidth of 10 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services. The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 2 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires a cross-connection for physical interconnect (colocation or carrier).

500247 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 2 - 25Mbps

Company's Responsibilities and Included Features

Description:
The Layer-2 E-Line service provides an Ethernet circuit, interconnecting carrier hotel to Company colocation facilities.

Service details:

- Managed transport services with a capped bandwidth of 25 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services. The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.

- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 2 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires a cross-connection for physical interconnect (colocation or carrier).

500248 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 2 - 50Mbps

Company's Responsibilities and Included Features

Description:
The Layer-2 E-Line service provides an Ethernet circuit, interconnecting carrier hotel to Company colocation facilities.

Service details:

- Managed transport services with a capped bandwidth of 50 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services. The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 2 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires a cross-connection for physical interconnect (colocation or carrier).

500249 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 2 - 100Mbps

Company's Responsibilities and Included Features

Description:
The Layer-2 E-Line service provides an Ethernet circuit, interconnecting carrier hotel to Company colocation facilities.

Service details:

- Managed transport services with a capped bandwidth of 100 Mbps.
  The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.

- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services. The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 2 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires a cross-connection for physical interconnect (colocation or carrier).

500250 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 2 - 200Mbps

Company's Responsibilities and Included Features

Description:
The Layer-2 E-Line service provides an Ethernet circuit, interconnecting carrier hotel to Company colocation facilities.

Service details:

- Managed transport services with a capped bandwidth of 200 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services. The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 2 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires a cross-connection for physical interconnect (colocation or carrier).

500251 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 2 - 500Mbps

Company's Responsibilities and Included Features

Description:
The Layer-2 E-Line service provides an Ethernet circuit, interconnecting carrier hotel to Company colocation facilities.

Service details:

- Managed transport services with a capped bandwidth of 500 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services. The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 2 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires a cross-connection for physical interconnect (colocation or carrier).

500252 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 2 - 1000Mbps

Company's Responsibilities and Included Features

Description:
The Layer-2 E-Line service provides an Ethernet circuit, interconnecting carrier hotel to Company colocation facilities.

Service details:

- Managed transport services with a capped bandwidth of 1000 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed and delivered over redundant routes, with non-redundant physical interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services. The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least one instance of this service and at least one instance of a layer 2 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
  Manage termination equipment infrastructure.

- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires a cross-connection for physical interconnect (colocation or carrier).

500253 ReliaCloud Connection Service - 1 Gbps

Company's Responsibilities and Included Features

Description:
ReliaCloud Connection Service delivers 1 Gbps layer 3 connectivity services between ReliaCloud and WAN termination devices in the telecommunications rooms or collocated cabinet(s) within Company data centers. The service provides up to two physical connections to provide path and infrastructure diversity into ReliaCloud. The service is designed to offer an extension of infrastructure services from ReliaCloud to colocation cabinets or a WAN circuit. The connection is layer 3 based to prevent conflicts with switching convergence.

Service details:

- Provide managed LAN services which provides speeds up to 1 Gbps.
- Provide all physical cabling to interconnect the hosted device to the ReliaCloud switching infrastructure.
- Deliver services over Cat5 or greater RJ-45 Ethernet
- Design, manage and maintain VLAN configuration.
- Maintain Access Control Lists (ACL's).
- Notify Client of any performance challenges or link-state issues with the service.
- Provide monitoring statics on port speed and performance.
- Service is not designed for Internet Routing table.
- Service does not provide VPN termination.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Provide physical device/s for termination of service.
- Ensure device/s support 1 Gbps RJ-45 Ethernet interfaces.

500254 ReliaCloud Connection Service - 10 Gbps

Company's Responsibilities and Included Features

Description:
ReliaCloud Connection Service delivers 10 Gbps layer 3 connectivity services between ReliaCloud and WAN termination devices in the telecommunications rooms or collocated cabinet(s) within Company data centers. The service provides up to two physical connections to provide path and infrastructure diversity into ReliaCloud. The service is designed to offer an extension of infrastructure services from ReliaCloud to colocation cabinets or a WAN circuit. The connection is layer 3 based to prevent conflicts with switching convergence.

Service details:

- Provide managed LAN services which provides speeds up to 10 Gbps.
- Provide all physical cabling to interconnect the hosted device to the ReliaCloud switching infrastructure.
- Deliver services over CatG or greater RJ-45 Ethernet
- Design, manage and maintain VLAN configuration.

Maintain Access Control Lists (ACL's).

- Notify Client of any performance challenges or link-state issues with the service.
- Provide monitoring statics on port speed and performance.
- Service is not designed for Internet Routing table.
- Service does not provide VPN termination.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Provide physical device/s for termination of service.
- Ensure device/s support 1 Gbps RJ-45 Ethernet interfaces.

600357 OneNeck Connect for Data Centers - Layer 2 NR -1000 Mbps

Company's Responsibilities and Included Features

Description

The Layer-2 Non-Redundant E-Line service provides a non-diverse, non-redundant Ethernet circuit, interconnecting Company colocation environments, carriers in Company telecommunications rooms, and physical cross-connects to Company colocation environments or carrier hotels.

Service details:

- Managed transport services with a capped bandwidth of 1000 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed to cross a specific set of OneNeck backbone links between non-redundant physical interconnects at each service location.
- Scheduled maintenance or circuit failures along this path will temporarily interrupt the service.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of this service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

600370 OneNeck Connect for Data Centers - Layer 2 NR -25 Mbps

Company's Responsibilities and Included Features

Description

The Layer-2 Non-Redundant E-Line service provides a non-diverse, non-redundant Ethernet circuit, interconnecting Company colocation environments, carriers in Company telecommunications rooms, and physical cross-connects to Company colocation environments or carrier hotels.

Service details:

- Managed transport services with a capped bandwidth of 25 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed to cross a specific set of OneNeck backbone links between non-redundant physical interconnects at each service location.
- Scheduled maintenance or circuit failures along this path will temporarily interrupt the service.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of this service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

600371 OneNeck Connect for Data Centers - Layer 2 NR - 50 Mbps

Company's Responsibilities and Included Features

Description

The Layer-2 Non-Redundant E-Line service provides a non-diverse, non-redundant Ethernet circuit, interconnecting Company colocation environments, carriers in Company telecommunications rooms, and physical cross-connects to Company colocation environments or carrier hotels.

Service details:

- Managed transport services with a capped bandwidth of 50 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed to cross a specific set of OneNeck backbone links between non-redundant physical interconnects at each service location.
- Scheduled maintenance or circuit failures along this path will temporarily interrupt the service.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of this service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

600372 OneNeck Connect for Data Centers - Layer 2 NR - 10Mbps

Company's Responsibilities and Included Features

Description:

The Layer-2 Non-Redundant E-Line service provides a non-diverse, non-redundant Ethernet circuit, interconnecting Company colocation environments, carriers in Company telecommunications rooms, and physical cross-connects to Company colocation environments or carrier hotels.

Service details:

- Managed transport services with a capped bandwidth of 10 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed to cross a specific set of OneNeck backbone links between non-redundant physical interconnects at each service location.
- Scheduled maintenance or circuit failures along this path will temporarily interrupt the service.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.

- The service requires exactly two instances of a layer 2 OneNeck Connect for Data Centers NR service for an end to end connection as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires a cross-connection for physical interconnect (colocation or carrier).

600373 OneNeck Connect for Data Centers - Layer 2 NR - 100Mbps

Company's Responsibilities and Included Features

Description

The Layer-2 Non-Redundant E-Line service provides a non-diverse, non-redundant Ethernet circuit, interconnecting Company colocation environments, carriers in Company telecommunications rooms, and physical cross-connects to Company colocation environments or carrier hotels.

Service details:

- Managed transport services with a capped bandwidth of 100 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed to cross a specific set of OneNeck backbone links between non-redundant physical interconnects at each service location.
- Scheduled maintenance or circuit failures along this path will temporarily interrupt the service.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of this service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.

- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

600374 OneNeck Connect for Data Centers - Layer 2 NR - 200Mbps

Company's Responsibilities and Included Features

Description

The Layer-2 Non-Redundant E-Line service provides a non-diverse, non-redundant Ethernet circuit, interconnecting Company colocation environments, carriers in Company telecommunications rooms, and physical cross-connects to Company colocation environments or carrier hotels.

Service details:

- Managed transport services with a capped bandwidth of 200 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 200 Mbps and 1 Gbps.
- The service is designed to cross a specific set of OneNeck backbone links between non-redundant physical interconnects at each service location.
- Scheduled maintenance or circuit failures along this path will temporarily interrupt the service.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of this service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

600375 OneNeck Connect for Data Centers - Layer 2 NR - 500Mbps

Company's Responsibilities and Included Features

Description

The Layer-2 Non-Redundant E-Line service provides a non-diverse, non-redundant Ethernet circuit, interconnecting Company colocation environments, carriers in Company telecommunications rooms, and physical cross-connects to Company colocation environments or carrier hotels.

Service details:

- Managed transport services with a capped bandwidth of 500 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 200 Mbps and 1 Gbps.
- The service is designed to cross a specific set of OneNeck backbone links between non-redundant physical interconnects at each service location.
- Scheduled maintenance or circuit failures along this path will temporarily interrupt the service.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of this service as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

600376 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 2 NR - 10Mbps

Company's Responsibilities and Included Features

Description:

The Layer-2 Non-Redundant E-Line service provides a non-diverse, non-redundant Ethernet circuit, interconnecting carrier hotel to Company colocation facilities.

Service details:

- Managed transport services with a capped bandwidth of 10 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed to cross a specific set of OneNeck backbone links between non-redundant physical interconnects at each service location.
- Scheduled maintenance or circuit failures along this path will temporarily interrupt the service.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).

- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of a layer 2 OneNeck Connect for Data Centers NR service for an end to end connection as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires a cross-connection for physical interconnect (colocation or carrier).

600378 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 2 NR - 25Mbps

Company's Responsibilities and Included Features

Description:

The Layer-2 Non-Redundant E-Line service provides a non-diverse, non-redundant Ethernet circuit, interconnecting carrier hotel to Company colocation facilities.

Service details:

- Managed transport services with a capped bandwidth of 25 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed to cross a specific set of OneNeck backbone links between non-redundant physical interconnects at each service location.
- Scheduled maintenance or circuit failures along this path will temporarily interrupt the service.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of a layer 2 OneNeck Connect for Data Centers NR service for an end to end connection as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.

- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires a cross-connection for physical interconnect (colocation or carrier).

600379 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 2 NR - 50Mbps

Company's Responsibilities and Included Features

Description:

The Layer-2 Non-Redundant E-Line service provides a non-diverse, non-redundant Ethernet circuit, interconnecting carrier hotel to Company colocation facilities.

Service details:

- Managed transport services with a capped bandwidth of 50 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed to cross a specific set of OneNeck backbone links between non-redundant physical interconnects at each service location.
- Scheduled maintenance or circuit failures along this path will temporarily interrupt the service.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of a layer 2 OneNeck Connect for Data Centers NR service for an end to end connection as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires a cross-connection for physical interconnect (colocation or carrier).

600380 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 2 NR - 100Mbps

Company's Responsibilities and Included Features

Description:

The Layer-2 Non-Redundant E-Line service provides a non-diverse, non-redundant Ethernet circuit, interconnecting carrier hotel to Company colocation facilities.

Service details:

- Managed transport services with a capped bandwidth of 100 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed to cross a specific set of OneNeck backbone links between non-redundant physical interconnects at each service location.
- Scheduled maintenance or circuit failures along this path will temporarily interrupt the service.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of a layer 2 OneNeck Connect for Data Centers NR service for an end to end connection as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires a cross-connection for physical interconnect (colocation or carrier).

600381 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 2 NR - 200Mbps

Company's Responsibilities and Included Features

Description:

The Layer-2 Non-Redundant E-Line service provides a non-diverse, non-redundant Ethernet circuit, interconnecting carrier hotel to Company colocation facilities.

Service details:

- Managed transport services with a capped bandwidth of 200 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed to cross a specific set of OneNeck backbone links between non-redundant physical interconnects at each service location.
- Scheduled maintenance or circuit failures along this path will temporarily interrupt the service.

Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of a layer 2 OneNeck Connect for Data Centers NR service for an end to end connection as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires a cross-connection for physical interconnect (colocation or carrier).

600382 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 2 NR - 500Mbps

Company's Responsibilities and Included Features

Description:

The Layer-2 Non-Redundant E-Line service provides a non-diverse, non-redundant Ethernet circuit, interconnecting carrier hotel to Company colocation facilities.

Service details:

- Managed transport services with a capped bandwidth of 500 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed to cross a specific set of OneNeck backbone links between non-redundant physical interconnects at each service location.
- Scheduled maintenance or circuit failures along this path will temporarily interrupt the service.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of a layer 2 OneNeck Connect for Data Centers NR service for an end to end connection as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires a cross-connection for physical interconnect (colocation or carrier).

600383 OneNeck Connect for Data Centers - Carrier Hotel Extensions - Layer 2 NR - 1000Mbps

Company's Responsibilities and Included Features

Description:

The Layer-2 Non-Redundant E-Line service provides a non-diverse, non-redundant Ethernet circuit, interconnecting carrier hotel to Company colocation facilities.

Service details:

- Managed transport services with a capped bandwidth of 1000 Mbps.
- The port size for the circuit is 1 Gbps, for service speed tiers between 10 Mbps and 1 Gbps.
- The service is designed to cross a specific set of OneNeck backbone links between non-redundant physical interconnects at each service location.
- Scheduled maintenance or circuit failures along this path will temporarily interrupt the service.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 2 pseudo-wire private connection, meaning no other customer can see or share the traffic on the same service segment.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires exactly two instances of a layer 2 OneNeck Connect for Data Centers NR service for an end to end connection as this service is only accounting for one side of a connection.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.
- The service requires a cross-connection for physical interconnect (colocation or carrier).

600434 Carrier Cross-Connection: Ethernet

Company's Responsibilities and Included Features

The cross connection service delivers a physical connection from the Data Center Telecommunications rooms to the Client Cloud demarcation point.

- Single physical cable delivered structured cable plant to the Client demarcation point.
- Category 5e, Adapter Interface RJ-45
- Support of cable and terminations
- Maintain on-site inventory or replacement materials (cable and connectors)
- Maintenance and protection of cable pathways

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Order and maintain circuit with vendor of choice
- Provide end termination equipment
- Provide circuit identification Numbers

600436 Carrier Cross-Connection: Fiber Optic Cross-Connect

Company's Responsibilities and Included Features

The cross connection service delivers a physical connection from the Data Center Telecommunications rooms to the Client demarcation point.

- Single physical cable delivered structured cable plant to the Client demarcation point.
- Singlemode Fiber, UPC/LC
- Support of cable and terminations
- Maintain on-site inventory or replacement materials (cable and connectors)
- Maintenance and protection of cable fiber pathways

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Order and maintain circuit with vendor of choice
- Provide end termination equipment
- Provide circuit identification Numbers

602831 OneNeck Connect Managed Circuit Service MKE 949N To MSN

Definitions:

MKE 949N: Milwaukee County circuit termination end point located at 949 N 9th St, Milwaukee Wisconsin.

Vendor: Third-party telecommunications carrier or service provider

Company's Responsibilities and Included Features

Description

The OneNeck Connect Managed Circuit Service -MKE 949N Service to MSN, provides a 10 Gbps, Layer 2 circuit between the MKE 949N location and Company MSN colocation facilities.

Service Details:

- Company will manage and maintain a point-to-point WAN service delivery from a Vendor. Company maintains the right to change Vendors with notification to Client.

- Port size is 10 Gbps
- Service speed is up to 10 Gbps
- Service is delivered as a layer 2 network service and provides no routing on its own

Service Exclusions:

- The Service is delivered as non-redundant. Scheduled maintenance or circuit failures along this path will temporarily interrupt the Service.
- Service does not provide any encryption level features

Service Management Details:

- Hold and maintain contract for Vendor s services on Client s behalf
- Act as the primary point of contact for Vendor s services
- Manage Vendor relations
- Provide notification to Client of any link-state issues with the service.
- For installation, maintenance, and repair, provide and coordinate with Vendor and Client escorted access to the carrier room or service demarcation point in
- Company s MSN data center, as well as Client premises.
- Identify outages and escalate to Vendor by opening trouble ticket
- Escalate trouble tickets with Vendor following Company standard operating procedure as defined within the Client Operations Handbook.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID

- Provide termination and routing equipment for the Service
- Manage termination and routing equipment infrastructure.
- Provide remote hands-on support if physical intervention is required for Service troubleshooting on Client premises.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access to Vendor and Company
- Ensure termination equipment has throughput capacity to support the service speeds.
- Notify Company if any service performance issues or failures occur. Company is your single point of contract for Vendor services.

602832 OneNeck Connect Managed Circuit Service MKE 821W To EDP

Definitions:

MKE 821W: Milwaukee County circuit termination end point located at 821 W. State St, Milwaukee Wisconsin.

Vendor: Third-party telecommunications carrier or service provider

Company's Responsibilities and Included Features

Description

The OneNeck Connect Managed Circuit Service -MKE 821W Service to EDP, provides a 10 Gbps, Layer 2 circuit between the MKE 821W location and Company EDP colocation facilities.

Service Details:

- Company will manage and maintain a point-to-point WAN service delivery from a Vendor. Company maintains the right to change Vendors with notification to Client.
- Port size is 10 Gbps
- Service speed is up to 10 Gbps
- Service is delivered as a layer 2 network service and provides no routing on its own

Service Exclusions:

- The Service is delivered as non-redundant. Scheduled maintenance or circuit failures along this path will temporarily interrupt the Service.
- Service does not provide any encryption level features

Service Management Details:

- Hold and maintain contract for Vendor s services on Client s behalf
- Act as the primary point of contact for Vendor s services
- Manage Vendor relations
- Provide notification to Client of any link-state issues with the service.
- For installation, maintenance, and repair, provide and coordinate with Vendor and Client escorted access to the carrier room or service demarcation point in
- Company s MSN data center, as well as Client premises.
- Identify outages and escalate to Vendor by opening trouble ticket
- Escalate trouble tickets with Vendor following Company standard operating procedure as defined within the Client Operations Handbook.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID

- Provide termination and routing equipment for the Service
- Manage termination and routing equipment infrastructure.
- Provide remote hands-on support if physical intervention is required for Service troubleshooting on Client premises.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access to Vendor and Company
- Ensure termination equipment has throughput capacity to support the service speeds.
- Notify Company if any service performance issues or failures occur. Company is your single point of contract for Vendor services.

602833 OneNeck Connect Managed Circuit Service EDP to MSN

Company's Responsibilities and Included Features

Description

The OneNeck Connect Managed Circuit Service EDP to MSN Service provides a 10 Gbps, Layer 2 circuit between Compnay EDP and MSN colocation facilities.

Service Details:

- Company will manage and maintain a point-to-point WAN service delivery from a Vendor. Company maintains the right to change Vendors with notification to Client.
- Port size is 10 Gbps
- Service speed is up to 10 Gbps
- Service is delivered as a layer 2 network service and provides no routing on its own

Service Exclusions:

- The Service is delivered as non-redundant. Scheduled maintenance or circuit failures along this path will temporarily interrupt the Service.
- Service does not provide any encryption level features

Service Management Details:

- Hold and maintain contract for Vendor s services on Client s behalf
- Act as the primary point of contact for Vendor s services
- Manage Vendor relations
- Provide notification to Client of any link-state issues with the service.
- For installation, maintenance, and repair, provide and coordinate with Vendor and Client escorted access to the carrier

room or service demarcation point in Company s MSN and EDP data centers.
- Identify outages and escalate to Vendor by opening trouble ticket
- Escalate trouble tickets with Vendor following Company standard operating procedure as defined within the Client Operations Handbook.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID

- Provide termination and routing equipment for the Service
- Manage termination and routing equipment infrastructure.
- Provide remote hands-on support if physical intervention is required for Service troubleshooting on Client premises.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access to Vendor and Company
- Ensure termination equipment has throughput capacity to support the service speeds.
- Notify Company if any service performance issues or failures occur. Company is your single point of contract for Vendor services.

604179 ReliaCloud Connection Service - 10 Gbps

Company's Responsibilities and Included Features

Description:
ReliaCloud Connection Service delivers 10 Gbps layer 3 connectivity services between ReliaCloud and WAN termination devices in the telecommunications rooms or collocated cabinet(s) within Company data centers. The service provides up to two physical connections to provide path and infrastructure diversity into ReliaCloud. The service is designed to offer an extension of infrastructure services from ReliaCloud to colocation cabinets or a WAN circuit. The connection is layer 3 based to prevent conflicts with switching convergence.

Service details:

- Provide managed LAN services which provides speeds up to 10 Gbps.
- Provide all physical cabling to interconnect the hosted device to the ReliaCloud switching infrastructure.
- Deliver services over CatG or greater RJ-45 Ethernet
- Design, manage and maintain VLAN configuration.
- Maintain Access Control Lists (ACL's).
- Notify Client of any performance challenges or link-state issues with the service.
- Provide monitoring statics on port speed and performance.
- Service is not designed for Internet Routing table.
- Service does not provide VPN termination.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at Client end of the service.
- Manage termination equipment infrastructure.
- Provide physical device/s for termination of service.
- Ensure device/s support 1 Gbps RJ-45 Ethernet interfaces.

604186 OneNeck Connect for Data Centers - Layer 3 - 10Gbps

Company's Responsibilities and Included Features

Description:
The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocation environments or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.

Service details:

- Managed transport services with a committed bandwidth of 10 Gbps.
- The port or virtual port size for the circuit is 10 Gbps, for service speed tiers up to 10 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection to any ReliaCloud workload.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least two instances of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 3 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

606802 OneNeck Connect for Data Centers - Layer 3 - 5000Mbps

Company's Responsibilities and Included Features

Description

The Layer-3 VPN (virtual private network) service (L3VPN) provides an IP VPN, interconnecting customer ReliaCloud environments, Company colocation environments, telecommunications MPLS clouds, and physical cross-connects to Company colocation environments or carrier hotels. Both static and Border Gateway Protocol (BGP) routing are supported.>

Service Details

- Managed transport services with a committed bandwidth of 5000 Mbps.
- The port or virtual port size for the circuit is 10 Gbps, for service speed tiers up to 10 Gbps.
- The service is designed and delivered over redundant routes, with redundant physical or virtual interconnects at each service location.
- Service delivery support on Cat5e (Copper) or Fiber.
- Service does not provide any encryption level services.
- The service is a layer 3 private connection, meaning no other customer can see or share the traffic on the same service segment.
- Service supports 9000 byte layer 3 IP frames.
- The service includes a cross-connection to any ReliaCloud workload.
- The service requires a cross-connection for any physical interconnect (colocation or carrier).
- Provide notification to Client of any performance challenges or link-state issues with the service.
- The service requires at least two instances of a layer 3 OneNeck Connect for Data Centers service as this service is only accounting for one side of a connection. Using this method, 3 or more Company data centers can be included in the L3VPN mesh with disparate bandwidths.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide termination equipment at both ends of the service if not ReliaCloud connected.
- Manage termination equipment infrastructure.
- Ensure termination equipment supports Ethernet service delivery.
- Ensure termination equipment has throughput capacity to support the contract service speeds.
- For the purposes of (up to intrusive) troubleshooting, provide physical or administrative level access.

Category: Disaster Recovery

110020-N ReliaCloud Recovery - Replication and Recovery License

Company's Responsibilities and Included Features

- Setup of replication process per virtual machine.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide access to administrative level access to production virtual machine for product installation.

110025 Avamar Grid to Grid

Company's Responsibilities and Included Features

- Supported Data Types:
  - Client hosted Avamar Grids
- Work with Client to configure Client grid replication to ReliaCloud grid
- Work with Client identify replication sets
- Configuration of replication security and user levels of access
- Backups processed from the Client grid environment to Company backup storage grid
- Exception reporting and notifications reviewed on a daily basis
- Client viewable backup reports posted to Company service desk portal
- Grid replication monitoring, reporting and notification
- Advanced administration support for backup infrastructure issues including triage of backup failures
- Support for initiating backup restorations (standard support SLA based on ticket severity)
- Restoration options:
  - Windows OS file level and bare metal restore
  - Non-Windows OS file level restore only
- Company provided engineering support for software upgrades as dictated by server side application software
- Initial configuration of grid replications and backend infrastructure components
- All subsequent adds/moves and changes to the grid replication and backend backup infrastructure including inclusions and exclusions from backup
- Backup infrastructure stored in Company secure ReliaCloud facility with proper 'chain of custody' tracking of all Client proprietary assets

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Custom backup job definitions (i.e. define what to backup when and how)
- Notify Company of all critical data locations or any changes to applications and proprietary data not already included in the current backup job definitions
- Review backup reports posted to Company service desk portal to ensure all expected backup jobs are occurring and complying with contracted data limit

- Backups of any systems/data not specifically covered by this item ID (i.e. servers not being managed by Company)

110028 Agent Based Cloud Backup 30

Company's Responsibilities and Included Features

- Recommended for under 2TB of backup
- Supported data types:
  - Network files systems
  - File servers
  - Databases
  - Virtual machines
  - Operating systems
  - Images
- Work with Client to install and configure agent on supported operating systems
- Configure 30 day retention policy
- Configuration of agent security and user levels of access
- Backups processed from the Client environment to Company backup storage infrastructure
- Exception reporting and notifications reviewed on a daily basis
- Client viewable backup reports posted to Company service desk portal
- Backup job monitoring, reporting and notification
- Advanced administration support for backup infrastructure issues including triage of backup failures
- Support for initiating backup restorations (standard support SLA based on ticket severity)
- Restoration options:
  - Windows OS file level and bare metal restore
  - Non-Windows OS file level restore only
- Company provided engineering support for agent software upgrades as dictated by server side application software
- Initial configuration of agent software and backend infrastructure components
- All subsequent adds/moves and changes to the agent and backend backup infrastructure including inclusions and exclusions from backup
- Backup infrastructure stored in Company secure ReliaCloud facility with proper 'chain of custody' tracking of all Client proprietary assets

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Custom backup job definitions (i.e. define what to backup when and how)
- Notify Company of all critical data locations or any changes to applications and proprietary data not already included in the current backup job definitions
- Review backup reports posted to Company service desk portal to ensure all expected backup jobs are occurring and complying with contracted data limit
- Backups of any systems/data not specifically covered by this item ID (i.e. servers not being managed by Company)

110029 Agent Based Cloud Backup 45

Company's Responsibilities and Included Features

- Recommended for under 2 TB of backup
- Supported data types:
  - Network files systems
  - File servers

        - Databases
        - Virtual machines
        - Operating systems
        - Images
    - Work with Client to install and configure agent on supported operating systems
    - Configure 45 day retention policy
    - Configuration of agent security and user levels of access
    - Backups processed from the Client environment to Company backup storage infrastructure
    - Exception reporting and notifications reviewed on a daily basis
    - Client viewable backup reports posted to Company service desk portal
    - Backup job monitoring, reporting and notification
    - Advanced administration support for backup infrastructure issues including triage of backup failures
    - Support for initiating backup restorations (standard support SLA based on ticket severity)
    - Restoration options:
        - Windows OS file level and bare metal restore
        - Non-Windows OS file level restore only
    - Company provided engineering support for agent software upgrades as dictated by server side application software
    - Initial configuration of agent software and backend infrastructure components
    - All subsequent adds/moves and changes to the agent and backend backup infrastructure including inclusions and exclusions from backup
    - Backup infrastructure stored in Company secure ReliaCloud facility with proper 'chain of custody' tracking of all Client proprietary assets

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Custom backup job definitions (i.e. define what to backup when and how)
- Notify Company of all critical data locations or any changes to applications and proprietary data not already included in the current backup job definitions
- Review backup reports posted to Company service desk portal to ensure all expected backup jobs are occurring and complying with contracted data limit
- Backups of any systems/data not specifically covered by this item ID (i.e. servers not being managed by Company)

110030 Agent Based Cloud Backup 60

Company's Responsibilities and Included Features

- Recommended for under 2 TB of backup
- Supported data types:
    - Network files systems
    - File servers
    - Databases
    - Virtual machines
    - Operating systems
    - Images
- Work with Client to install and configure agent on supported operating systems
- Configure 60 day retention policy
- Configuration of agent security and user levels of access
- Backups processed from the Client environment to Company backup storage infrastructure

- Exception reporting and notifications reviewed on a daily basis
- Client viewable backup reports posted to Company service desk portal
- Backup job monitoring, reporting and notification
- Advanced administration support for backup infrastructure issues including triage of backup failures
- Support for initiating backup restorations (standard support SLA based on ticket severity)
- Restoration options:
    - Windows OS file level and bare metal restore
    - Non-Windows OS file level restore only
- Company provided engineering support for agent software upgrades as dictated by server side application software
- Initial configuration of agent software and backend infrastructure components
- All subsequent adds/moves and changes to the agent and backend backup infrastructure including inclusions and exclusions from backup
- Backup infrastructure stored in Company secure ReliaCloud facility with proper 'chain of custody' tracking of all Client proprietary assets

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Custom backup job definitions (i.e. define what to backup when and how)
- Notify Company of all critical data locations or any changes to applications and proprietary data not already included in the current backup job definitions
- Review backup reports posted to Company service desk portal to ensure all expected backup jobs are occurring and complying with contracted data limit
- Backups of any systems/data not specifically covered by this item ID (i.e. servers not being managed by Company)

600254 Custom Runbook for RTO of specified devices

Company's Responsibilities and Included Features

Company shall execute the steps contained within a jointly designed Runbook by Company and Client to facilitate a disaster recovery sequence.

Execution of Runbook

- Execute Runbook sequence as initiated by Client
- Complete Runbook sequence by the 12 hour Recovery Time Objective (RTO)
    - Runbook RTO time is calculated after notification by Client

Maintenance of Runbook

- Provide updates to the documentation as necessary
- Maintain Runbook within the Company Service Portal

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Specify which devices or systems need to be part of the Runbook
- Contract for managed services of those specified devices
- Notify Company of any changes in scope
- Provide contact and escalation points
- Notify Company of the need to execute the Runbook

600272 DRaaS - Virtual Replication Service licensing (per VM) setup

Company's Responsibilities and Included Features

- Initial configuration of Virtual Replication Service
- Requires: 600597 - Disaster Recovery Software as a Service with Management - Dedicated monthly service
- Troubleshooting support for Virtual Replication Service application and functionality
- Provide access to management portal to test and initiate disaster recovery activities

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Declaration of "Disaster" and Virtual Replication Service fail-over initiation
- Provide additional compute and network resources required to support Virtual Replication Service infrastructure
- Disaster Recovery testing and/or testing simulation

600548 Agent Based Cloud Backup 90

Company's Responsibilities and Included Features

Description

The Agent-Based Cloud Backup 90 service provides desktop or server level remote back up. The service Agent runs locally on the Customer's equipment and sends the backup data to the Client's ReliaCloud storage infrastructure. This nighly transaction is facilitated by a Customer provided internet connection to the location being serviced.

- Recommended for under 2 TB of backup
- Supported data types:
    - Network files systems
    - File servers
    - Databases
    - Virtual machines
    - Operating systems
    - Images
- Work with Client to install and configure agent on supported operating systems
- Configure 90-day retention policy
    - Nightly file backup
- Configuration of agent security and user levels of access
- Backups processed from the Client environment to Company backup storage infrastructure
- Exception reporting and notifications reviewed on a daily basis
- Backup job monitoring, reporting, and notification
- Advanced administration support for backup infrastructure issues including triage of backup failures
- Support for initiating backup restorations (standard support SLA based on ticket severity)

- Restoration options:
    - Windows OS
    - File-level and bare metal restore Non-Windows OS
    - File-level restore only
- Company provided engineering support for agent software upgrades as dictated by server-side application software
- Initial configuration of agent software and backend infrastructure components
    - All subsequent adds/moves and changes to the agent and backend backup infrastructure including inclusions and exclusions from backup
- Backup infrastructure stored in Company secure ReliaCloud facility with proper 'chain of custody' tracking of all Client proprietary asset

Backup Metering

- This is a metered service.
- Protected data is defined as the size of the data protected from the server that is being backed up.
- The size of the protected data is measured by the size of the largest full, uncompressed, un-deduplicated backup, during the billing period, as measured by the backup system. The unit of measurement is protected GB.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Definition of what needs to be backed up
- Define the window of time within which the backup may be initiated
- Operating system administration of servers being backed up
- Installation and management of backup agents on servers being backed up if local agents are required
- Validation of data restored

601448

Company's Responsibilities and Included Features

Company will provide access to a multi-tenant Dell/EMC Data Domain for the purpose of acting as a secondary storage target within a designated ReliaCloud Pod location. The service is delivered as a metered service allowing Client to consume the storage in a pay-as-you-go model. The service solution is designed to integrate with a client provided geographically diverse primary Dell/EMC Data Domain, over a Client provide WAN link to the designated ReliaCloud Pod location.

Service Management

- Work with Client to configure source appliance replication to ReliaCloud Data Domain target infrastructure
- Work with Client to identify replication sets
    - Configuration of replication security and user levels of access
    - Initial configuration of backend infrastructure components
    - Initial and ongoing configuration of replication sets
- Monitor and maintain Company Data Domain and associated infrastructure
- Report on client storage space usage

Supported Data Types

- Client hosted Data Domain appliances (no NAS support)
- Supports only MTree (no directory or collection replication scenarios)
- Supports VTL MTrees for offsite copy only (no local SAN access)

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for replication errors, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General operating system level troubleshooting
  - Escalation to the hardware provider
- To resolve system incidents, Company will:
  - Apply Company known solutions
  - Apply replication hardware/software vendor provided solutions
  - Document user issues and system errors
- Company will triage and manage the troubleshooting process for replication errors.

Service Metering

- This is a metered service.
- The size of the stored data is measured as the largest peak size in GB during the month stored on the Appliance. Data stored equals the amount of Data stored on Company s Data Domain. The billing period for this service is monthly, as measured by the backup system. The unit of measurement is GB stored, rounded-up to the nearest whole GB.

Service Level Agreement

- SLA for Appliance availability is 99.99%

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client Infrastructure

- Procurement and management of Client owned primary Dell/EMC Data Domain
- Procurement and management of WAN infrastructure to support the replication process
- Open any necessary ports and conduits between the primary Dell/EMC Data Domain and ReliaCloud Data Domain target
- Provide Company with access, passwords, access codes or security devices as necessary to perform the services

Replication and Backup Management

- Backups of any systems/data not specifically covered by this item ID (i.e. servers not being managed by Company)
- Define data to be replicated via policy
- Define retention period on Company Data Domain
- Resources for restoring data are outside the scope of this service
- Provide restoration environment and restoration resources including backup software in DR location
- Connectivity to Company environment
- Management of Client backup software
- Management of Client s source Data Domain
- Avamar management (if part of replication environment)

Category: Disaster Recovery as a Service

606990 ReliaCloud DRaaS Internet Service Available Bandwidth

Company's Responsibilities and Included Features

Company will provide a redundant, multi-provider, managed Internet Bandwidth service (Service) to provide high performance, highly available internet access. Company will load balance traffic over multiple upstream Internet transit providers. The Service is provided via the ReliaCloud network, no physical hand-offs are provided.

- Service may be capped up to the maximum allocation size indicated on the service order.

Service may also leverage ReliaCloud DRaaS Internet Service - Burstable Bandwidth ItemID 606991, calculated on the 95% of peak usage
- Deliver committed Internet bandwidth allocation in 1 Mbps increments
- At Client's request, Company will support integration with Client provided BGP routing schema. Configuration of this activiity will be billed as a scoped, time and materials engagment via a seperate SoW.
- Provide access to upstream and downstream bandwidth usage graphs via Company portal

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- ReliaCloud Internet Service - Committed Bandwidth is an unsecured raw Internet connection. Client is responsible for providing virtual or physical security appliances or contracting with Company for Internet security services such as but not limited to; firewalls, intrusion detection, security incident and response management (SIEM), denial of service prevention, and traffic filtering. Note that providing physical infrastructure may require the use of additional company ItemIDs.
- Comply with Acceptable Use Policy (AUP) https://www.oneneck.com/acceptable-use-policy
- Notify Company if additional bandwidth is needed beyond the committed allocation

606991 ReliaCloud DRaaS Internet Service Burstable Bandwidth

Company's Responsibilities and Included Features

Cloud Internet Burstable Service is add-on component to Item ID 606990 ReliaCloud DRaaS Internet Service Available Bandwidth.

- Clients will have a default maximum burst capacity of 1 Gbps.
- Bandwidth utilization in excess of the Available Bandwidth will be billed as Burstable Bandwidth and calculated using the 95th Percentile Method, in 1 Mbps increments.

This service is a metered service

The 95th Percentile Method involves polling both inbound and outbound bandwidth utilization every five (5) minutes during each calendar month. All such samples are ordered from highest to lowest. The top 5 percent of readings are discarded, and Client is billed an additional charge based on the next highest reading. The amount of contracted available Bandwidth is subtracted from the 95th Percentile to determine the Burstable Bandwidth usage to be billed. Aditional Available Bandwidth is billed in advance; Burstable Bandwidth is billed in arrears, the month after usage occurs. By requesting a hard limit higher than the Available Bandwidth, Client agrees to be subject to the Burstable Bandwidth for bandwidth consumed beyond the Committed Bandwidth rate level on a monthly basis.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- ReliaCloud Internet Service - Burstable Bandwidth is an unsecured raw Internet connection. Client is responsible for providing virtual or physical security appliances or contracting with Company for Internet security services such as but not limited to; firewalls, intrusion detection, security incident and response management (SIEM), denial of service prevention, and traffic filtering. Note that providing physical infrastructure may require the use of additional company ItemIDs.
- Comply with Acceptable Use Policy (AUP) https://www.oneneck.com/acceptable-use-policy

607075 Managed Cisco Adaptive Security Virtual Appliance for DRaaS (ASAv10)

The Managed Cisco Adaptive Security Virtual Appliance Model 10 (Managed ASAv10) service is a combination of Company managed services for a firewall and Cisco software licensing for the purpose of running a single (non-redundant) ASAv10 firewall on a ReliaCloud Disaster Recovery as a Service (DRaaS) environments which is separately contracted with Company, to provide VPN and firewalling for DRaaS environments.

Definitions

Intellectual Property: any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Feature Specification

The following table provides the ASAv10 feature specifications that Company will manage:

Feature	**Entitlement / Managed Support**	**Licensing Included**
Stateful inspection firewall throughput (maximum) *	1 Gbps	Yes
Stateful inspection firewall throughput (multiprotocol) **	500 Mbps	Yes
Advanced Encryption Standard (AES) VPN throughput***	750 Mbps	Yes
Connections per second	20,000	Yes
Concurrent sessions	100,000	Yes
VLANs	50	Yes
Bridge groups	25	Yes
IPsec VPN peers****	25	Yes
Cisco AnyConnect or clientless VPN user sessions*****	250	Yes

Note: Cisco s Cisco Adaptive Security Virtual Appliance v10 may include software features not listed in the table above. Any unlisted services are not within the scope of Company s managed support of virtual appliance.

*Maximum throughput measured by Cisco with User Datagram Protocol (UDP) traffic under ideal conditions.

** Multiprotocol refers to a traffic profile consisting primarily of TCP-based protocols or applications like HTTP, SMTP, FTP, IMAPv4, BitTorrent, and DNS.

*** The VPN throughput and the number of sessions depend on the ASA device configuration and VPN traffic patterns. These elements should be taken into consideration as part of your capacity planning.

**** Note, additional IPSec VPN peers (>25) are available and can be purchased from Company under a separate ItemID.

*****Cisco AnyConnect or clientless VPN user sessions are not included with this ItemID, but can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Scope of Usage

- Provides a VPN tunnel endpoint for Client s to connect to the DRaaS environment. This will be for:
  - Management connectivity between the Client s Nutanix cluster and the DRaaS cluster
  - Disaster recovery data replication traffic
  - Client user access into the DRaaS environment
  - Client may also elect Use this firewall as a primary firewall for workloads running in DRaaS
- Contracting this model of Security Virtual Appliance and its associated throughput capacity is not a guarantee by the Company that the capacity is sufficient for Client s needs

Firewall Management

- Configuration of address translation (NAT/PAT)
- Configuration of firewall rule management
- Virtualization cluster configuration support (if needed)
- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of Cisco AnyConnect including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing Cisco client software
    - Site-to-site VPN management
        - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
        - Troubleshooting / support of VPN tunnel establishment

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the ASAv5 software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

End of Support

The Cisco ASAv10 is subject to an EOS Date, as described above in this SOW.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Intellectual Property in and to the Services belonging to Cisco or other Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide virtualizing resources to meet or exceed the Managed ASAv10 Infrastructure specifications.
    - Minimum virtualized resources necessary to run the Managed ASAv10 are as follows:
        - 2 vCPU
        - 4 GB memory *
        - 8 GB storage

* Up to 8 GB of memory is required to support 50 Cisco AnyConnect User Sessions

- Provide and configure desired internal and external network services
- Open any necessary ports and conduits between the Appliance and Company s management services
- Specify and implement, desired fault tolerance. Note, the Managed ASAv10 is a single (1) virtual appliance and non-redundant. Should Client desire fault tolerance from a fail-over, reboot, or system maintenance window, a second (2 total) Managed ASAv10 should be deployed and configured for high-availability. That service is available from Company under a separate ItemID.
- Client is responsible for performing all Security Operations Center (SOC) services including but not limited to:
    - Security incident response
    - Security incident identification, analysis, defense, investigation and reporting
    - Data breach investigation and reporting
    - Security gap analysis
    - Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco ASAv10 software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf and the Cisco Secure Supplemental End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/anyconnect-SEULA-v4x.pdf (collectively the Cisco Terms).

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at OneNeck or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Intellectual Property rights including pursuing an action against any breaching third parties.

607090 ReliaCloud DRaaS Node DRS.2486H

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud DRaaS Node DRS.2486H (DRaaS Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV dedicated to providing a Disaster Recovery (DR) target for Client s Nutanix Clusters. This includes the ability to host active workloads necessary for DR. DRaaS Nodes minimally belong to a Cluster configured with at least three (3) DRaaS Nodes. DRaaS Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide a DRaaS Node that meets or exceeds the following physical specifications:

- 24 cores
- 768 GB RAM
- Hybrid disk configuration of 72 TB HDD and 15.36 TB of NVMe storage

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an DRaaS Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI Ultimate
- Nutanix NCM PRO
- Nutanix Calm
- Nutanix Flow Network Security

The DRaaS Node includes the following Nutanix software that can be self-enrolled and disenrolled by Customer. Usage of this software may incur additional charges as defined by the Agreement:

- Nutanix Files License Service - AOS Per TiB
- Nutanix Objects License Service - AOS Per TiB

Cluster and Node Setup:

- Company will setup and configure a private DRaaS Cluster with quantity of nodes contracted.

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication

Erasure coding (EC-X) *

- Nutanix Volumes Management
  - Creation of iSCSI volume group(s)
  - Management of volume groups
  - Management of client iSCSI initiators
  - Management of iSCSI data services
  - Configure Bare Metal Nodes for IP addressing
  - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
  - Data path redundancy
  - Tunable redundancy factor
- Security
  - Client authentication
  - Cluster lockdown
  - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
  - Prism Central and Prism Elements
  - PulseCluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node maintenance management is limited to:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

Cluster Network Administration

Company will provide the following Cluster network activities to enable DR testing and failover.

During a DR Test

- If the systems being failed over will not undergo reassignment of IPs, Company will need to change the routing for Nutanix Guest Tools (NGT) prior to executing a DR test
    - Company requires at least 24 hours advanced notice of a DR test being conducted by the Client. This notification is to be through a ticket into the Company Service Desk
- If the systems being failed over will undergo reassignment of IPs, then no Company executed network changes are required

During a DR Failover

- If the systems being failed over will not undergo reassignment of IPs, Company will need to activate the DR network as it would be in a deactivated state so as to not conflict with the existing production network prior to executing a DR failover
    - Client to request this through a P1 ticket into the Company Service Desk
- If the systems being failed over will undergo reassignment of IPs, then no Company executed network changes are required

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client s notification of Updates
- Application of Updates during Company s defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s

discretion and in accordance with standard industry practices.

Expert User Technical Support:

Technical support may only be requested by a Client s Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Administration

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features are available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
  - Cluster and VM performance and analysis
  - Cluster, health and availability
  - Cluster capacity and trend info
  - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
  - Create, delete and modify VMs
  - Execute snapshots and restorations
  - Add VMs to catalog
  - Import, add, create and delete images to catalog
  - Create and modify data protection policies and recovery plans

Network Administration during Testing or Failover

During a DR Test

- If the systems being failed over will not undergo reassignment of IPs, Company will need to change the routing for Nutanix Guest Tools (NGT) prior to executing a DR test
  - Client is required to submit a ticket into the Company Service Desk at least 24 hours in advanced of a DR test being conducted by the Client to re-route the NGT network traffic
- Access into the isolated test network. Typically provided by a Client provided jump box which can be accessed for the DR network but has connectivity into the DR network

During a DR Failover

- If the systems being failed over will not undergo reassignment of IPs, Company will need to activate the DR network as it would be in a deactivated state so as to not conflict with the existing production network prior to executing a DR failover
  - Client to request this through a P1 ticket into the Company Service Desk
- External or Wide Area Network (WAN) failover

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup

- Manage network devices
- Migrate physical machines and/or VMs onto or off the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment
- This platform includes software features that are Customer discoverable and allow for self-enrollment. These services are metered usage and will bill monthly based upon their usage. The following ItemIDs must be subscribed to, but don't require their use unless desired by Customer:
    - 606611 Nutanix Files License Service - AOS Per TiB
    - 606612 Nutanix Objects License Service - AOS Per TiB

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / DR Plan:

- Client business continuity plan(s) and DR plan(s) are solely Client s responsibilities and are out of scope for this engagement.
- Setup and management of Nutanix Protection Policies
- Setup and management of Nutanix Recovery Plans
- Initiation and management of failover process
- DR testing

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees and acknowledges, and understands that any Nutanix licensing component of this service is subject to price changes by Nutanix and that these changes may be passed on to the Client as and when Nutanix informs Company of price changes
- Client agrees that Nutanix offerings provided herein are subject to, and governed by, the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula , which is hereby incorporated into this SOW in full

607091 ReliaCloud DRaaS Node DRS.2486H-Reserved

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud DRaaS Node DRS.2486H-Reserved (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications:

Company will provide a DRaaS Node that meets or exceeds the following physical specifications:

- 24 cores
- 768 GB RAM
- Hybrid disk configuration of 72 TB HDD and 15.36 TB of NVMe storage

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud DRaaS Activated Reserved Node Rate, until Client submits a service request for an Activated Reserved Node to be removed from the Cluster, at which point the Reserved Node will revert to its Reserved Node billing rate

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is four (4) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud DRaaS Advanced Node DRS.2486H Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud DRaaS Advanced Node DRS.2486H-Activated Reserved Services
- Notify Company to request Node activation, deactivation or changes in use to production status

607092 ReliaCloud DRaaS Node DRS.2486H-Reserved Activated

Company's Responsibilities and Included Features

ReliaCloud DRaaS Node DRS.2486H-Reserved Activated (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. An Activated Node is a ReliaCloud DRaaS Node DRS.2486H-Reserved Node that has been joined to an existing Cluster at Client request and is available for Client s use.

A ReliaCloud DRaaS Node DRS.2486H-Reserved Activated is identical to ReliaCloud DRaaS Node DRS.2486H, except the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company responsibilities, included features, Client responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed monthly in whole day increments for each day that it is activated until Client submits a service request for the Activated Node to be removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud DRaaS Node DRS.2486H Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud DRaaS Node DRS.2486H-Reserved Services

607093 ReliaCloud DRaaS Node DRS.3676N

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud DRaaS Node DRS.3676N (DRaaS Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV dedicated to providing a Disaster Recovery (DR) target for Client s Nutanix Clusters. This includes the ability to host active workloads necessary for DR. DRaaS Nodes minimally belong to a Cluster configured with at least three (3) DRaaS Nodes. DRaaS Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide a DRaaS Node that meets or exceeds the following physical specifications:

- 36 cores
- 1024 GB RAM
- 76.8 TB of NVMe storage

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an DRaaS Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI Ultimate
- Nutanix NCM PRO
- Nutanix Calm
- Nutanix Flow Network Security

The DRaaS Node includes the following Nutanix software that can be self-enrolled and disenrolled by Customer. Usage of this software may incur additional charges as defined by the Agreement:

- Nutanix Files License Service - AOS Per TiB
- Nutanix Objects License Service - AOS Per TiB

Cluster and Node Setup:

- Company will setup and configure a private DRaaS Cluster with quantity of nodes contracted.

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
-
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
-
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
    - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
-
    - Data path redundancy
    - Tunable redundancy factor
- Security
-
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
-
    - Prism Central and Prism Elements
    - PulseCluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node maintenance management is limited to:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
-
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
-
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
-
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

Cluster Network Administration

Company will provide the following Cluster network activities to enable DR testing and failover.

During a DR Test

- If the systems being failed over will not undergo reassignment of IPs, Company will need to change the routing for Nutanix Guest Tools (NGT) prior to executing a DR test
    - Company requires at least 24 hours advanced notice of a DR test being conducted by the Client. This notification is to be through a ticket into the Company Service Desk
- If the systems being failed over will undergo reassignment of IPs, then no Company executed network changes are required

During a DR Failover

- If the systems being failed over will not undergo reassignment of IPs, Company will need to activate the DR network as

it would be in a deactivated state so as to not conflict with the existing production network prior to executing a DR failover
    - Client to request this through a P1 ticket into the Company Service Desk
- If the systems being failed over will undergo reassignment of IPs, then no Company executed network changes are required

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client s notification of Updates
- Application of Updates during Company s defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Expert User Technical Support:

Technical support may only be requested by a Client s Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Administration

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features are available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
-
    - Cluster and VM performance and analysis
    - Cluster, health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
-
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection policies and recovery plans

Network Administration during Testing or Failover

During a DR Test

- If the systems being failed over will not undergo reassignment of IPs, Company will need to change the routing for Nutanix Guest Tools (NGT) prior to executing a DR test
    - Client is required to submit a ticket into the Company Service Desk at least 24 hours in advanced of a DR test being conducted by the Client to re-route the NGT network traffic
- Access into the isolated test network. Typically provided by a Client provided jump box which can be accessed for the DR network but has connectivity into the DR network

During a DR Failover

- If the systems being failed over will not undergo reassignment of IPs, Company will need to activate the DR network as it would be in a deactivated state so as to not conflict with the existing production network prior to executing a DR failover
    - Client to request this through a P1 ticket into the Company Service Desk
- External or Wide Area Network (WAN) failover

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment
- This platform includes software features that are Customer discoverable and allow for self-enrollment. These services are metered usage and will bill monthly based upon their usage. The following ItemIDs must be subscribed to, but don't require their use unless desired by Customer:
-
    - 606611 Nutanix Files License Service - AOS Per TiB
    - 606612 Nutanix Objects License Service - AOS Per TiB

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / DR Plan:

- Client business continuity plan(s) and DR plan(s) are solely Client s responsibilities and are out of scope for this engagement.
- Setup and management of Nutanix Protection Policies
- Setup and management of Nutanix Recovery Plans
- Initiation and management of failover process
- DR testing

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees and acknowledges, and understands that any Nutanix licensing component of this service is subject to price changes by Nutanix and that these changes may be passed on to the Client as and when Nutanix informs Company of price changes
- Client agrees that Nutanix offerings provided herein are subject to, and governed by, the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula , which is hereby incorporated into this SOW in full

607094 ReliaCloud DRaaS Node DRS.3676N-Reserved

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud DRaaS Node DRS.3676N-Reserved (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications:

Company will provide a DRaaS Node that meets or exceeds the following physical specifications:

- 36 cores
- 1024 GB RAM
- 76.8 TB of NVMe storage

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud DRaaS Activated Reserved Node Rate, until Client submits a service request for an Activated Reserved Node to be removed from the Cluster, at which point the Reserved Node will revert to its Reserved Node billing rate

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is four (4) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud DRaaS Advanced Node DRS.3676N Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud DRaaS Advanced Node DRS.3676N-Activated Reserved Services
- Notify Company to request Node activation, deactivation or changes in use to production status

607095 ReliaCloud DRaaS Node DRS.3676N-Reserved Activated

Company's Responsibilities and Included Features

ReliaCloud DRaaS Node DRS.3676N-Reserved Activated (Activated Node) service is comprised of hardware, software and a

base level of management services for the Nutanix AOS and Nutanix AHV. An Activated Node is a ReliaCloud DRaaS Node DRS.3676N-Reserved Node that has been joined to an existing Cluster at Client request and is available for Client s use.

A ReliaCloud DRaaS Node DRS.3676N-Reserved Activated is identical to ReliaCloud DRaaS Node DRS.3676N, except the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company responsibilities, included features, Client responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed monthly in whole day increments for each day that it is activated until Client submits a service request for the Activated Node to be removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud DRaaS Node DRS.3676N Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud DRaaS Node DRS.3676N-Reserved Services

607096 ReliaCloud DRaaS Starter Node DRS.1230N

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud DRaaS Starter Node DRS.1230N (DRaaS Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV, dedicated to providing a Disaster Recovery (DR) target for Client s Nutanix Clusters. This includes the ability to host active workloads necessary for DR. Starter DRaaS Nodes Clusters are limited to a minimum of three (3) DRaaS Nodes per Clusters. DRaaS Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide a DRaaS Node that meets or exceeds the following physical specifications:

- 12 cores
- 512 GB RAM
- 30.72 TB of NVMe storage

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an DRaaS Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI Ultimate
- Nutanix NCM PRO
- Nutanix Calm
- Nutanix Flow Network Security

The DRaaS Node includes the following Nutanix software that can be self-enrolled and disenrolled by Customer. Usage of this software may incur additional charges as defined by the Agreement:

- Nutanix Files License Service - AOS Per TiB
- Nutanix Objects License Service - AOS Per TiB

Cluster and Node Setup:

- Company will setup and configure a private DRaaS Cluster with quantity of nodes contracted.

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
-
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
-
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
    - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
-
    - Data path redundancy
    - Tunable redundancy factor
- Security
-
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
-
    - Prism Central and Prism Elements
    - PulseCluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all

configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node maintenance management is limited to:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
-
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
-
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
-
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles

- VM high availability
- Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

Cluster Network Administration

Company will provide the following Cluster network activities to enable DR testing and failover.

During a DR Test

- If the systems being failed over will not undergo reassignment of IPs, Company will need to change the routing for Nutanix Guest Tools (NGT) prior to executing a DR test
  - Company requires at least 24 hours advanced notice of a DR test being conducted by the Client. This notification is to be through a ticket into the Company Service Desk
- If the systems being failed over will undergo reassignment of IPs, then no Company executed network changes are required

During a DR Failover

- If the systems being failed over will not undergo reassignment of IPs, Company will need to activate the DR network as it would be in a deactivated state so as to not conflict with the existing production network prior to executing a DR failover
  - Client to request this through a P1 ticket into the Company Service Desk
- If the systems being failed over will undergo reassignment of IPs, then no Company executed network changes are required

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client s notification of Updates
- Application of Updates during Company s defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Expert User Technical Support:

Technical support may only be requested by a Client s Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Administration

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features are available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
-
    - Cluster and VM performance and analysis
    - Cluster, health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
-
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection policies and recovery plans

Network Administration during Testing or Failover

During a DR Test

- If the systems being failed over will not undergo reassignment of IPs, Company will need to change the routing for Nutanix Guest Tools (NGT) prior to executing a DR test
    - Client is required to submit a ticket into the Company Service Desk at least 24 hours in advanced of a DR test being conducted by the Client to re-route the NGT network traffic
- Access into the isolated test network. Typically provided by a Client provided jump box which can be accessed for the DR network but has connectivity into the DR network

During a DR Failover

- If the systems being failed over will not undergo reassignment of IPs, Company will need to activate the DR network as it would be in a deactivated state so as to not conflict with the existing production network prior to executing a DR failover
    - Client to request this through a P1 ticket into the Company Service Desk
- External or Wide Area Network (WAN) failover

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment
- This platform includes software features that are Customer discoverable and allow for self-enrollment. These services are metered usage and will bill monthly based upon their usage. The following ItemIDs must be subscribed to, but don't require their use unless desired by Customer:
-
    - 606611 Nutanix Files License Service - AOS Per TiB
    - 606612 Nutanix Objects License Service - AOS Per TiB

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / DR Plan:

- Client business continuity plan(s) and DR plan(s) are solely Client s responsibilities and are out of scope for this engagement.
- Setup and management of Nutanix Protection Policies
- Setup and management of Nutanix Recovery Plans
- Initiation and management of failover process
- DR testing

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees and acknowledges, and understands that any Nutanix licensing component of this service is subject to price changes by Nutanix and that these changes may be passed on to the Client as and when Nutanix informs Company of price changes
- Client agrees that Nutanix offerings provided herein are subject to, and governed by, the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula , which is hereby incorporated into this SOW in full

607101 Internet IP Address Range for ReliaCloud /29 Allocation (8 addresses) for DRaaS

Company's Responsibilities and Included Features

- Provide an Internet routable IPv4 subnet /29 address range
- The address range provides 8 subnet addresses. Note that usable address space within that subnet will vary depending on network routing schema and Client terminating equipment, physical or virtual.
- Maintain Internet routing tables
- Company provided IPv4 address space is not portable or transferrable to another carrier
- Maintain documentation for the IP network with the RIR (e.g. ARIN).
- Enforce IP conservation policies
- Company reserves the right to reclaim any unused address space or space that is not supplied with proper ARIN documentation.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide justification documentation for IP compliance requirements from the American Registry for Internet Numbers (ARIN).
- Stay within ARIN's usage compliance requirements

607102 ReliaCloud DRaaS Node DRS.2486H-LO Reserved Activated

Company's Responsibilities and Included Features

ReliaCloud DRaaS Node DRS.2486H-LO Reserved Activated (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. An Activated Node is a ReliaCloud DRaaS Node DRS.2486H-Reserved Node that has been joined to an existing Cluster at Client request and is available for Client s use.

A ReliaCloud DRaaS Node DRS.2486H-LO Reserved Activated is identical to ReliaCloud DRaaS Node DRS.2486H, except the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company responsibilities, included features, Client responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed monthly in whole day increments for each day that it is activated until Client submits a service request for the Activated Node to be removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud DRaaS Node DRS.2486H Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud DRaaS Node DRS.2486H-Reserved Services

607103 ReliaCloud DRaaS Node DRS.3676N-LO Reserved Activated

Company's Responsibilities and Included Features

ReliaCloud DRaaS Node DRS.3676N-LO Reserved Activated (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. An Activated Node is a ReliaCloud DRaaS Node DRS.3676N-Reserved Node that has been joined to an existing Cluster at Client request and is available for Client s use.

A ReliaCloud DRaaS Node DRS.3676N-LO Reserved Activated is identical to ReliaCloud DRaaS Node DRS.3676N, except the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company responsibilities, included features, Client responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed monthly in whole day increments for each day that it is activated until Client submits a service request for the Activated Node to be removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud DRaaS Node DRS.3676N Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud DRaaS Node DRS.3676N-Reserved Services

608407 ReliaCloud DRaaS Node DRS.1230N-Reserved

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud DRaaS Node DRS.1230N-Reserved (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications:

Company will provide a DRaaS Node that meets or exceeds the following physical specifications:

- 12 cores
- 512 GB RAM
- 30.72 TB of NVMe storage

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud DRaaS Activated Reserved Node Rate, until Client submits a service request for an Activated Reserved Node to be removed from the Cluster, at which point the Reserved Node will revert to its Reserved Node billing rate

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is four (4) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW

611268 ReliaCloud DRaaS Node DRS.2486H

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud DRaaS Node DRS.2486H (DRaaS Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV dedicated to providing a Disaster Recovery (DR) target for Client s Nutanix Clusters. This includes the ability to host active workloads necessary for DR. DRaaS Nodes minimally belong to a Cluster configured with at least three (3) DRaaS Nodes. DRaaS Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide a DRaaS Node that meets or exceeds the following physical specifications:

- 24 cores
- 768 GB RAM
- Hybrid disk configuration of 72 TB HDD and 15.36 TB of NVMe storage

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an DRaaS Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI Ultimate
- Nutanix NCM PRO
- Nutanix Calm
- Nutanix Flow Network Security

The DRaaS Node includes the following Nutanix software that can be self-enrolled and disenrolled by Customer. Usage of this software may incur additional charges as defined by the Agreement:

- Nutanix Files License Service - AOS Per TiB
- Nutanix Objects License Service - AOS Per TiB

Cluster and Node Setup:

- Company will setup and configure a private DRaaS Cluster with quantity of nodes contracted.

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
    - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - PulseCluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node maintenance management is limited to:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

Cluster Network Administration

Company will provide the following Cluster network activities to enable DR testing and failover.

During a DR Test

- If the systems being failed over will not undergo reassignment of IPs, Company will need to change the routing for Nutanix Guest Tools (NGT) prior to executing a DR test
    - Company requires at least 24 hours advanced notice of a DR test being conducted by the Client. This notification is to be through a ticket into the Company Service Desk
- If the systems being failed over will undergo reassignment of IPs, then no Company executed network changes are required

During a DR Failover

- If the systems being failed over will not undergo reassignment of IPs, Company will need to activate the DR network as it would be in a deactivated state so as to not conflict with the existing production network prior to executing a DR failover
    - Client to request this through a P1 ticket into the Company Service Desk
- If the systems being failed over will undergo reassignment of IPs, then no Company executed network changes are required

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client s notification of Updates
- Application of Updates during Company s defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Expert User Technical Support:

Technical support may only be requested by a Client s Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Administration

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features are available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
    - Cluster and VM performance and analysis
    - Cluster, health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards

- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection policies and recovery plans

Network Administration during Testing or Failover

During a DR Test

- If the systems being failed over will not undergo reassignment of IPs, Company will need to change the routing for Nutanix Guest Tools (NGT) prior to executing a DR test
    - Client is required to submit a ticket into the Company Service Desk at least 24 hours in advanced of a DR test being conducted by the Client to re-route the NGT network traffic
- Access into the isolated test network. Typically provided by a Client provided jump box which can be accessed for the DR network but has connectivity into the DR network

During a DR Failover

- If the systems being failed over will not undergo reassignment of IPs, Company will need to activate the DR network as it would be in a deactivated state so as to not conflict with the existing production network prior to executing a DR failover
    - Client to request this through a P1 ticket into the Company Service Desk
- External or Wide Area Network (WAN) failover

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment
- This platform includes software features that are Customer discoverable and allow for self-enrollment. These services are metered usage and will bill monthly based upon their usage. The following ItemIDs must be subscribed to, but don't require their use unless desired by Customer:
    - 606611 Nutanix Files License Service - AOS Per TiB
    - 606612 Nutanix Objects License Service - AOS Per TiB

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / DR Plan:

- Client business continuity plan(s) and DR plan(s) are solely Client s responsibilities and are out of scope for this engagement.
- Setup and management of Nutanix Protection Policies
- Setup and management of Nutanix Recovery Plans
- Initiation and management of failover process
- DR testing

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees and acknowledges, and understands that any Nutanix licensing component of this service is subject to

price changes by Nutanix and that these changes may be passed on to the Client as and when Nutanix informs Company of price changes

- Client agrees that Nutanix offerings provided herein are subject to, and governed by, the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula , which is hereby incorporated into this SOW in full

611391 ReliaCloud DRaaS Node DRS.4892N

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud DRaaS Node DRS.4892N (DRaaS Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV dedicated to providing a Disaster Recovery (DR) target for Client s Nutanix Clusters. This includes the ability to host active workloads necessary for DR. DRaaS Nodes minimally belong to a Cluster configured with at least three (3) DRaaS Nodes. DRaaS Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide a DRaaS Node that meets or exceeds the following physical specifications:

- 48 cores
- 1024 GB RAM
- 92.16 TB of NVMe storage

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an DRaaS Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI Ultimate
- Nutanix NCM PRO
- Nutanix Calm
- Nutanix Flow Network Security

The DRaaS Node includes the following Nutanix software that can be self-enrolled and disenrolled by Customer. Usage of this software may incur additional charges as defined by the Agreement:

- Nutanix Files License Service - AOS Per TiB
- Nutanix Objects License Service - AOS Per TiB

Cluster and Node Setup:

- Company will setup and configure a private DRaaS Cluster with quantity of nodes contracted.

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
-
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
-
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
    - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
-
    - Data path redundancy
    - Tunable redundancy factor
- Security
-
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
-
    - Prism Central and Prism Elements
    - PulseCluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows

- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node maintenance management is limited to:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
-
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
-
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
-
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

Cluster Network Administration

Company will provide the following Cluster network activities to enable DR testing and failover.

During a DR Test

- If the systems being failed over will not undergo reassignment of IPs, Company will need to change the routing for Nutanix Guest Tools (NGT) prior to executing a DR test
    - Company requires at least 24 hours advanced notice of a DR test being conducted by the Client. This notification is to be through a ticket into the Company Service Desk
- If the systems being failed over will undergo reassignment of IPs, then no Company executed network changes are

required

During a DR Failover

- If the systems being failed over will not undergo reassignment of IPs, Company will need to activate the DR network as it would be in a deactivated state so as to not conflict with the existing production network prior to executing a DR failover
    - Client to request this through a P1 ticket into the Company Service Desk
- If the systems being failed over will undergo reassignment of IPs, then no Company executed network changes are required

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client s notification of Updates
- Application of Updates during Company s defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Expert User Technical Support:

Technical support may only be requested by a Client s Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Administration

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features are available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
-
    - Cluster and VM performance and analysis
    - Cluster, health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
-
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog

- Create and modify data protection policies and recovery plans

Network Administration during Testing or Failover

During a DR Test

- If the systems being failed over will not undergo reassignment of IPs, Company will need to change the routing for Nutanix Guest Tools (NGT) prior to executing a DR test
  - Client is required to submit a ticket into the Company Service Desk at least 24 hours in advanced of a DR test being conducted by the Client to re-route the NGT network traffic
- Access into the isolated test network. Typically provided by a Client provided jump box which can be accessed for the DR network but has connectivity into the DR network

During a DR Failover

- If the systems being failed over will not undergo reassignment of IPs, Company will need to activate the DR network as it would be in a deactivated state so as to not conflict with the existing production network prior to executing a DR failover
  - Client to request this through a P1 ticket into the Company Service Desk
- External or Wide Area Network (WAN) failover

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment
- This platform includes software features that are Customer discoverable and allow for self-enrollment. These services are metered usage and will bill monthly based upon their usage. The following ItemIDs must be subscribed to, but don't require their use unless desired by Customer:
-
  - 606611 Nutanix Files License Service - AOS Per TiB
  - 606612 Nutanix Objects License Service - AOS Per TiB

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / DR Plan:

- Client business continuity plan(s) and DR plan(s) are solely Client s responsibilities and are out of scope for this engagement.
- Setup and management of Nutanix Protection Policies
- Setup and management of Nutanix Recovery Plans
- Initiation and management of failover process
- DR testing

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees and acknowledges, and understands that any Nutanix licensing component of this service is subject to price changes by Nutanix and that these changes may be passed on to the Client as and when Nutanix informs Company of price changes
- Client agrees that Nutanix offerings provided herein are subject to, and governed by, the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula , which is hereby incorporated into this SOW in full

611392 ReliaCloud DRaaS Node DRS.4892N-Reserved

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud DRaaS Node DRS.4892N-Reserved (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications:

Company will provide a DRaaS Node that meets or exceeds the following physical specifications:

- 48 cores
- 1024 GB RAM
- 92.16 TB of NVMe storage

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud DRaaS Activated Reserved Node Rate, until Client submits a service request for an Activated Reserved Node to be removed from the Cluster, at which point the Reserved Node will revert to its Reserved Node billing rate

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is four (4) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud DRaaS Advanced Node DRS.4892N Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud DRaaS Advanced Node DRS.4892N-Activated Reserved Services
- Notify Company to request Node activation, deactivation or changes in use to production status

611393 ReliaCloud DRaaS Node DRS.4892N-Reserved Activated

Company's Responsibilities and Included Features

ReliaCloud DRaaS Node DRS.4892N-Reserved Activated (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. An Activated Node is a ReliaCloud DRaaS Node DRS.4892N-Reserved Node that has been joined to an existing Cluster at Client request and is available for Client s use.

A ReliaCloud DRaaS Node DRS.4892N-Reserved Activated is identical to ReliaCloud DRaaS Node DRS.4892N, except the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company responsibilities, included features, Client responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed monthly in whole day increments for each day that it is activated until Client submits a service request for the Activated Node to be removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud DRaaS Node DRS.4892N Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud DRaaS Node DRS.4892N-Reserved Services

Category: Internet

110002 Cloud Internet Burstable

Company's Responsibilities and Included Features

Cloud Internet Burstable Service is add-on component to Item ID 110001 Cloud Internet Committed Service.

- Clients will have a maximum burst capacity of 1 Gbps.
- Bandwidth utilization in excess of the Committed Bandwidth will be billed as Burstable Bandwidth and calculated using the 95th Percentile Method, in 1 Mbps increments.

The 95th Percentile Method involves polling both inbound and outbound bandwidth utilization every five (5) minutes during each calendar month. All such samples are ordered from highest to lowest. The top 5 percent of readings are discarded, and Client is billed an additional charge based on the next highest reading. The amount of pre-purchased Committed Bandwidth is subtracted from the 95th Percentile to determine the Burstable Bandwidth usage to be billed. Committed Bandwidth is billed in advance; Burstable Bandwidth is billed in arrears, the month after usage occurs. By requesting a hard limit higher than the Committed Bandwidth, Client agrees to be subject to the Burstable Bandwidth for bandwidth consumed beyond the Committed Bandwidth rate level on a monthly basis.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Comply with Internet acceptable use policy
- Commit to at least 1 Mbps of Cloud Internet Committed bandwidth ItemID 110001

603300 ReliaCloud Internet Service Committed Bandwidth

Company's Responsibilities and Included Features

Company will provide a redundant, multi-provider, managed Internet Bandwidth service (Service) to provide high performance, highly available internet access. Company will load balance traffic over multiple upstream Internet transit providers. The Service is provided via the ReliaCloud network, no physical hand-offs are provided.

- Service may be capped up to the maximum allocation size indicated on the service order.
- Service may also leverage ReliaCloud Internet Service - Burstable Bandwidth ItemID 603301, calculated on the 95% of peak usage
- Deliver committed Internet bandwidth allocation in 1 Mbps increments
- Provide a base allocation of up to 3 usable via (/29 network) Internet routing IPv4 Public addresses, unless the Client provides their own ASN and IPv4 portable address space
- Company provided IPv4 address space is not portable or transferable to another carrier
- Client may procure additional Internet routing IPv4 Public addresses in network blocks under additional company ItemIDs.
- At Client's request, Company will support integration with Client provided BGP routing schema. Configuration of this activity will be billed as a scoped, time and materials engagement via a separate SoW.
- Provide access to upstream and downstream bandwidth usage graphs via Company portal

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- ReliaCloud Internet Service - Committed Bandwidth is an unsecured raw Internet connection. Client is responsible for providing virtual or physical security appliances or contracting with Company for Internet security services such as but not limited to; firewalls, intrusion detection, security incident and response management (SIEM), denial of service prevention, and traffic filtering. Note that providing physical infrastructure may require the use of additional company ItemIDs.
- Comply with Acceptable Use Policy (AUP) https://www.oneneck.com/acceptable-use-policy
- Notify Company if additional bandwidth is needed beyond the committed allocation
- Commit to at least 1 Mbps of committed Internet bandwidth

603301 ReliaCloud Internet Service Burstable Bandwidth

Company's Responsibilities and Included Features

ReliaCloud Internet Service -Burstable Bandwidth is add-on component to Item ID 603300 ReliaCloud Internet Service Committed Bandwidth.

- Clients will have a default maximum burst capacity of 1 Gbps.
- Bandwidth utilization in excess of the Committed Bandwidth will be billed as Burstable Bandwidth and calculated using the 95th Percentile Method, in 1 Mbps increments.

This service is a metered service

The 95th Percentile Method involves polling both inbound and outbound bandwidth utilization every five (5) minutes during each calendar month. All such samples are ordered from highest to lowest. The top 5 percent of readings are discarded, and Client is billed an additional charge based on the next highest reading. The amount of pre-purchased Committed Bandwidth is subtracted from the 95th Percentile to determine the Burstable Bandwidth usage to be billed. Committed Bandwidth is billed in advance; Burstable Bandwidth is billed in arrears, the month after usage occurs. By requesting a hard limit higher than the Committed Bandwidth, Client agrees to be subject to the Burstable Bandwidth for bandwidth consumed beyond the Committed Bandwidth rate level on a monthly basis.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- ReliaCloud Internet Service - Burstable Bandwidth is an unsecured raw Internet connection. Client is responsible for providing virtual or physical security appliances or contracting with Company for Internet security services such as but not limited to; firewalls, intrusion detection, security incident and response management (SIEM), denial of service prevention, and traffic filtering. Note that providing physical infrastructure may require the use of additional company ItemIDs.

- Comply with Acceptable Use Policy (AUP) https://www.oneneck.com/acceptable-use-policy
- Commit to at least 1 Mbps of ReliaCloud Internet Service - Committed Bandwith ItemID 603301

604177 ReliaCloud Internet Service Committed Bandwidth

Company's Responsibilities and Included Features

Company will provide a redundant, multi-provider, managed Internet Bandwidth service (Service) to provide high performance, highly available internet access. Company will load balance traffic over multiple upstream Internet transit providers. The Service is provided via the ReliaCloud network, no physical hand-offs are provided.

- Service may be capped up to the maximum allocation size indicated on the service order.
- Service may also leverage ReliaCloud Internet Service - Burstable Bandwidth ItemID 604177, calculated on the 95% of peak usage
- Deliver committed Internet bandwidth allocation in 1 Mbps increments
- Provide a base allocation of up to 3 usable via (/29 network) Internet routing IPv4 Public addresses, unless the Client provides their own ASN and IPv4 portable address space
- Company provided IPv4 address space is not portable or transferable to another carrier
- Client may procure additional Internet routing IPv4 Public addresses in network blocks under additional company ItemIDs.
- At Client's request, Company will support integration with Client provided BGP routing schema. Configuration of this activity will be billed as a scoped, time and materials engagement via a separate SoW.
- Provide access to upstream and downstream bandwidth usage graphs via Company portal

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- ReliaCloud Internet Service - Committed Bandwidth is an unsecured raw Internet connection. Client is responsible for providing virtual or physical security appliances or contracting with Company for Internet security services such as but not limited to; firewalls, intrusion detection, security incident and response management (SIEM), denial of service prevention, and traffic filtering. Note that providing physical infrastructure may require the use of additional company ItemIDs.
- Comply with Acceptable Use Policy (AUP) https://www.oneneck.com/acceptable-use-policy
- Notify Company if additional bandwidth is needed beyond the committed allocation
- Commit to at least 1 Mbps of committed Internet bandwidth

604178 ReliaCloud Internet Service Burstable Bandwidth

Company's Responsibilities and Included Features

ReliaCloud Internet Service -Burstable Bandwidth is add-on component to Item ID 604178 ReliaCloud Internet Service Committed Bandwidth.

- Clients will have a default maximum burst capacity of 1 Gbps.
- Bandwidth utilization in excess of the Committed Bandwidth will be billed as Burstable Bandwidth and calculated using the 95th Percentile Method, in 1 Mbps increments.

This service is a metered service

The 95th Percentile Method involves polling both inbound and outbound bandwidth utilization every five (5) minutes during each calendar month. All such samples are ordered from highest to lowest. The top 5 percent of readings are discarded, and Client is billed an additional charge based on the next highest reading. The amount of pre-purchased Committed Bandwidth is subtracted from the 95th Percentile to determine the Burstable Bandwidth usage to be billed. Committed Bandwidth is billed in advance; Burstable Bandwidth is billed in arrears, the month after usage occurs. By requesting a hard limit higher than the Committed Bandwidth, Client agrees to be subject to the Burstable Bandwidth for bandwidth consumed beyond the Committed Bandwidth rate level on a monthly basis.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- ReliaCloud Internet Service - Burstable Bandwidth is an unsecured raw Internet connection. Client is responsible for providing virtual or physical security appliances or contracting with Company for Internet security services such as but not limited to; firewalls, intrusion detection, security incident and response management (SIEM), denial of service prevention, and traffic filtering. Note that providing physical infrastructure may require the use of additional company ItemIDs.
- Comply with Acceptable Use Policy (AUP) https://www.oneneck.com/acceptable-use-policy
- Commit to at least 1 Mbps of ReliaCloud Internet Service - Committed Bandwith ItemID 604178

Category: IPv4 Address Space

110005 Additional IPv4 Internet Public Addresses Space

Company's Responsibilities and Included Features

Company provides a base allocation of IPv4 public addressable Internet address space with our committed Internet products. Clients may request additional address space to their base allocation, and additional IPs will indicated on the Service order. Company reserves the right to reclaim any unused address space, or space that is not supplied with proper ARIN documentation. Blocks of IP addresses can only be sold in quantities consistent with standard IP address bit boundaries (i.e. /30[4 IPs], /29 [8 IPs], /28 [16 IPs], 27 [32 IPs], 26 [64 IPs], 25 [128 IPs], 24 [256 IPs], etc)

- Provide additional allocations IPv4 publically routable Internet Address space.
- Maintain Internet routing tables
- Maintain all IP documentation
- Enforce IP conservation policies

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Comply and provide justification documentation with IP documentation requirements from the American Registry for Internet Numbers(ARIN)
- Request additional IPv4 Internet address as necessary.

603302 Internet IP Address Range for ReliaCloud /24 Allocation (256 addresses)

Company's Responsibilities and Included Features

- Provide an Internet routable IPv4 subnet /24 address range
- The address range provides 256 subnet addresses. Note that usable address space within that subnet will vary depending on network routing schema and Client terminating equipment, physical or virtual.
- Maintain Internet routing tables
- Company provided IPv4 address space is not portable or transferrable to another carrier
- Maintain documentation for the IP network with the RIR (e.g. ARIN).
- Enforce IP conservation policies
- Company reserves the right to reclaim any unused address space or space that is not supplied with proper ARIN documentation.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide justification documentation for IP compliance requirements from the American Registry for Internet Numbers (ARIN).
- Stay within ARIN's usage compliance requirements

603303 Internet IP Address Range for ReliaCloud /25 Allocation (128 addresses)

Company's Responsibilities and Included Features

- Provide an Internet routable IPv4 subnet /25 address range
- The address range provides 128 subnet addresses. Note that usable address space within that subnet will vary depending on network routing schema and Client terminating equipment, physical or virtual.
- Maintain Internet routing tables
- Company provided IPv4 address space is not portable or transferrable to another carrier
- Maintain documentation for the IP network with the RIR (e.g. ARIN).
- Enforce IP conservation policies
- Company reserves the right to reclaim any unused address space or space that is not supplied with proper ARIN documentation.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide justification documentation for IP compliance requirements from the American Registry for Internet Numbers (ARIN).
- Stay within ARIN's usage compliance requirements

603304 Internet IP Address Range for ReliaCloud /26 Allocation (64 addresses)

Company's Responsibilities and Included Features

- Provide an Internet routable IPv4 subnet /26 address range
- The address range provides 64 subnet addresses. Note that usable address space within that subnet will vary depending on network routing schema and Client terminating equipment, physical or virtual.
- Maintain Internet routing tables
- Company provided IPv4 address space is not portable or transferrable to another carrier
- Maintain documentation for the IP network with the RIR (e.g. ARIN).
- Enforce IP conservation policies
- Company reserves the right to reclaim any unused address space or space that is not supplied with proper ARIN documentation.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide justification documentation for IP compliance requirements from the American Registry for Internet Numbers (ARIN).
- Stay within ARIN's usage compliance requirements

603305 Internet IP Address Range for ReliaCloud /27 Allocation (32 addresses)

Company's Responsibilities and Included Features

- Provide an Internet routable IPv4 subnet /27 address range
- The address range provides 32subnet addresses. Note that usable address space within that subnet will vary depending on network routing schema and Client terminating equipment, physical or virtual.
- Maintain Internet routing tables
- Company provided IPv4 address space is not portable or transferrable to another carrier
- Maintain documentation for the IP network with the RIR (e.g. ARIN).
- Enforce IP conservation policies
- Company reserves the right to reclaim any unused address space or space that is not supplied with proper ARIN documentation.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide justification documentation for IP compliance requirements from the American Registry for Internet Numbers (ARIN).
- Stay within ARIN's usage compliance requirements

603306 Internet IP Address Range for ReliaCloud /28 Allocation (16 addresses)

Company's Responsibilities and Included Features

- Provide an Internet routable IPv4 subnet /28 address range
- The address range provides 16 subnet addresses. Note that usable address space within that subnet will vary depending on network routing schema and Client terminating equipment, physical or virtual.
- Maintain Internet routing tables
- Company provided IPv4 address space is not portable or transferrable to another carrier
- Maintain documentation for the IP network with the RIR (e.g. ARIN).
- Enforce IP conservation policies
- Company reserves the right to reclaim any unused address space or space that is not supplied with proper ARIN documentation.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide justification documentation for IP compliance requirements from the American Registry for Internet Numbers (ARIN).
- Stay within ARIN's usage compliance requirements

603307 Internet IP Address Range for ReliaCloud /29 Allocation (8 addresses)

Company's Responsibilities and Included Features

- Provide an Internet routable IPv4 subnet /29 address range
- The address range provides 8 subnet addresses. Note that usable address space within that subnet will vary depending on network routing schema and Client terminating equipment, physical or virtual.
- Maintain Internet routing tables
- Company provided IPv4 address space is not portable or transferrable to another carrier
- Maintain documentation for the IP network with the RIR (e.g. ARIN).
- Enforce IP conservation policies
- Company reserves the right to reclaim any unused address space or space that is not supplied with proper ARIN documentation.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide justification documentation for IP compliance requirements from the American Registry for Internet Numbers (ARIN).
- Stay within ARIN's usage compliance requirements

603308 Internet IP Address Range for ReliaCloud /30 Allocation (4 addresses)

Company's Responsibilities and Included Features

- Provide an Internet routable IPv4 subnet /30 address range
- The address range provides 4 subnet addresses. Note that usable address space within that subnet will vary depending on network routing schema and Client terminating equipment, physical or virtual.
- Maintain Internet routing tables
- Company provided IPv4 address space is not portable or transferrable to another carrier
- Maintain documentation for the IP network with the RIR (e.g. ARIN).
- Enforce IP conservation policies
- Company reserves the right to reclaim any unused address space or space that is not supplied with proper ARIN documentation.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide justification documentation for IP compliance requirements from the American Registry for Internet Numbers (ARIN).
- Stay within ARIN's usage compliance requirements

Category: Licensing CITRIX

601764 Citrix ADC VPX 10 Mbps Standard (CSP)

This ItemID 601764 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 10 Mbps Standard

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

601947 Citrix ADC VPX 200 Mbps Standard (CSP)

This ItemID 601947 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 200 Mbps Standard

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

602220 Citrix ADC VPX 200 Mbps Advanced (CSP)

This ItemID 602220 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by

Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 200 Mbps Standard

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

603562 Citrix DaaS Premium License Service - 1-2500 Users

Company's Responsibilities and Included Features

Citrix DaaS Premium License Service (Service) provides subscription access to Citrix Cloud Services on a per named user per month basis. The Service provides for any number of named users between 1 and up to 2500 named users. The Service is only for Citrix DaaS Premium services and it does not provide service management or hardware to run the services.

The Service provides features such as:

- Virtual apps and desktops
- Deliver multi and single-session Windows and Linux desktops
- Citrix app personlization
- Remote PC access to physical desktops
- Hybrid multi-cloud desktop provisioning
- Advanced image management tools
- Premium monitoring with historical reporting
- Session recording
- User performance and scalability enhancements
- Advanced security and adaptive authentication

More information can be found here https://www.citrix.com/products/citrix-daas/ or here https://www.citrix.com/products/citrix-daas/feature-matrix.html.

Metered Service

- This service is metered
- The number of users per month is calculated by the total number unique users that have logged into the Service for any period during the calendar month.

Term

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month-to-month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Provide or contract for end solution hardware and software
- Deployment and configuration of Citrix Cloud Software
- Management and operation of Citrix Cloud Software

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.
- Client agrees that Citrix offerings provided herein are subject to the Citrix License and Service Agreement available https://www.citrix.com/content/dam/citrix/en_us/documents/buy/enterprise-saas-eusa.pdf, which is hereby incorporated into this SOW in full.

603804 Citrix ADC VPX 1000 Mbps Standard (CSP)

This ItemID 603804 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 1000 Mbps Standard

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

603805 Citrix ADC VPX 3000 Mbps Standard (CSP)

This ItemID 603805 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 3000 Mbps Standard

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

None

603806 Citrix ADC VPX 5000 Mbps Standard (CSP)

This ItemID 603806 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 5000 Mbps Standard

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

603807 Citrix ADC VPX 8000 Mbps Standard (CSP)

This ItemID 603807 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 8000 Mbps Standard

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

603808 Citrix ADC VPX 10 Mbps Advanced (CSP)

This ItemID 603808 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 10 Mbps Advanced

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

603809 Citrix ADC VPX 1000 Mbps Advanced (CSP)

This ItemID 603809 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 1000 Mbps Advanced

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

603810 Citrix ADC VPX 3000 Mbps Advanced (CSP)

This ItemID 603810 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 3000 Mbps Advanced

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

603811 Citrix ADC VPX 5000 Mbps Advanced (CSP)

This ItemID 603811 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 5000 Mbps Advanced

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

603812 Citrix ADC VPX 8000 Mbps Advanced (CSP)

This ItemID 603812 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 8000 Mbps Advanced

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

603813 Citrix ADC VPX 10 Mbps Premium (CSP)

This ItemID 603813 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 10 Mbps Premium

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

603815 Citrix ADC VPX 200 Mbps Premium (CSP)

This ItemID 603815 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 200 Mbps Premium

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

603816 Citrix ADC VPX 1000 Mbps Premium (CSP)

This ItemID 603816 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 1000 Mbps Premium

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

603817 Citrix ADC VPX 3000 Mbps Premium (CSP)

This ItemID 603817 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 3000 Mbps Premium

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

603818 Citrix ADC VPX 5000 Mbps Premium (CSP)

This ItemID 603818 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 5000 Mbps Premium

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

603819 Citrix ADC VPX 8000 Mbps Premium (CSP)

This ItemID 603819 contains an order for licensing of software provided by Citrix Systems, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.

Client agrees that the Citrix Offerings are subject to the Citrix End User License Agreement available at https://www.citrix.com/buy/licensing/agreements.html and privacy policy located at https://www.citrix.com/about/legal/privacy/ , which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based Citrix software licensing for Citrix ADC VPX 8000 Mbps Premium

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

604406 Citrix DaaS Advanced Plus License Service - 1-2500 Users

Company's Responsibilities and Included Features

Citrix DaaS Advanced Plus License Service (Service) provides subscription access to Citrix Cloud Services on a per named user per month basis. The Service provides for any number of named users between 1 and up to 2500 named users. The Service is only for Citrix DaaS Advanced Plus services and it does not provide service management or hardware to run the services.

The Service provides features such as:

- Virtual apps and desktops
- Deliver single and multi-session Windows and Linux desktops
- Remote PC access to physical desktops
- Hybrid multi-cloud desktop provisioning
- Advanced image management tools
- Advanced monitoring with historical reporting
- Session recording
- User performance and scalability enhancements

More information can be found here https://www.citrix.com/products/citrix-daas/ or here https://www.citrix.com/products/citrix-daas/feature-matrix.html.

Metered Service

- This service is metered
- The number of users per month is calculated by the total number of unique users that have logged into the Service for any period during the calendar month.

Term

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month-to-month basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Provide or contract for end solution hardware and software
- Deployment and configuration of Citrix Cloud Software
- Management and operation of Citrix Cloud Software

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix

Systems, Inc.

- Client agrees that Citrix offerings provided herein are subject to the Citrix License and Service Agreement available https://www.citrix.com/content/dam/citrix/en_us/documents/buy/enterprise-saas-eusa.pdf, which is hereby incorporated into this SOW in full.

608971 Citrix Universal Hybrid Multi-Cloud License Service - Quarterly

Company's Responsibilities and Included Features

Citrix Universal Hybrid Multi-Cloud License Service provides subscription access to Citrix Cloud Services on a per user basis (see Citrix definition of user here: https://www.cloud.com/content/dam/cloud/documents/legal/business-unit-terms.pdf). The Service provides for a committed amount of users per year. The Service is only for Citrix Universal Hybrid Multi-Cloud services and it does not provide service management or hardware to run the services.

The Service provides features such as:

- Virtual apps and desktops
- Deliver multi and single-session Windows and Linux desktops
- Citrix app personlization
- Remote PC access to physical desktops
- Hybrid multi-cloud desktop provisioning
- Advanced image management tools
- Premium monitoring with historical reporting
- Session recording
- User performance and scalability enhancements
- Advanced security and adaptive authentication
- Netscaler instances and capacity

More information can be found here: https://www.citrix.com/platform/citrix-app-and-desktop-virtualization/feature-matrix.html.

Term

- Notwithstanding the term of this Statement of Work, this Offering is provided on a yearly basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Provide or contract for end solution hardware and software
- Deployment and configuration of Citrix Cloud Software
- Management and operation of Citrix Cloud Software

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.
- Client agrees that Citrix offerings provided herein are subject to the Citrix License and Service Agreement available https://www.citrix.com/content/dam/citrix/en_us/documents/buy/enterprise-saas-eusa.pdf, which is hereby incorporated into this SOW in full.

611098 Citrix Universal Hybrid Multi-Cloud License Service - Annual

Company's Responsibilities and Included Features

Citrix Universal Hybrid Multi-Cloud License Service provides subscription access to Citrix Cloud Services on a per user basis (see Citrix definition of user here: https://www.cloud.com/content/dam/cloud/documents/legal/business-unit-terms.pdf). The Service provides for a committed amount of users per year. The Service is only for Citrix Universal Hybrid Multi-Cloud services and it does not provide service management or hardware to run the services.

The Service provides features such as:

- Virtual apps and desktops
- Deliver multi and single-session Windows and Linux desktops
- Citrix app personlization
- Remote PC access to physical desktops
- Hybrid multi-cloud desktop provisioning
- Advanced image management tools
- Premium monitoring with historical reporting
- Session recording
- User performance and scalability enhancements
- Advanced security and adaptive authentication
- Netscaler instances and capacity

More information can be found here: https://www.citrix.com/platform/citrix-app-and-desktop-virtualization/feature-matrix.html.

Term

- Notwithstanding the term of this Statement of Work, this Offering is provided on a yearly basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Provide or contract for end solution hardware and software
- Deployment and configuration of Citrix Cloud Software
- Management and operation of Citrix Cloud Software

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.
- Client agrees that Citrix offerings provided herein are subject to the Citrix License and Service Agreement available https://www.citrix.com/content/dam/citrix/en_us/documents/buy/enterprise-saas-eusa.pdf, which is hereby incorporated into this SOW in full.

611267 Citrix Universal Hybrid Multi-Cloud License Service - Monthly

Company's Responsibilities and Included Features

Citrix Universal Hybrid Multi-Cloud License Service provides subscription access to Citrix Cloud Services on a per user basis (see Citrix definition of user here: https://www.cloud.com/content/dam/cloud/documents/legal/business-unit-terms.pdf). The Service provides for a committed amount of users per year. The Service is only for Citrix Universal Hybrid Multi-Cloud services and it does not provide service management or hardware to run the services.

The Service provides features such as:

- Virtual apps and desktops
- Deliver multi and single-session Windows and Linux desktops

Citrix app personlization
- Remote PC access to physical desktops
- Hybrid multi-cloud desktop provisioning
- Advanced image management tools
- Premium monitoring with historical reporting
- Session recording
- User performance and scalability enhancements
- Advanced security and adaptive authentication
- Netscaler instances and capacity

More information can be found here: https://www.citrix.com/platform/citrix-app-and-desktop-virtualization/feature-matrix.html.

Term

- Notwithstanding the term of this Statement of Work, this Offering is provided on a yearly basis.
- Company may revise terms of use or pricing to reflect changes by Citrix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Provide or contract for end solution hardware and software
- Deployment and configuration of Citrix Cloud Software
- Management and operation of Citrix Cloud Software

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Citrix offerings will be provided and made by Citrix Systems, Inc. and may be subject to change as determined by Citrix Systems, Inc.
- Client agrees that Citrix offerings provided herein are subject to the Citrix License and Service Agreement available https://www.citrix.com/content/dam/citrix/en_us/documents/buy/enterprise-saas-eusa.pdf, which is hereby incorporated into this SOW in full.

Category: Licensing Microsoft SPLA

601761 Microsoft Windows Server Datacenter (Core License) - 2 Core - Corporate - Lic/SA

This ItemID 601761 contains an order for Microsoft Corporation WinSvrDCCore ALNG LicSAPk MVL 2Lic CoreLic licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

601854 Microsoft Visio Standard - SAL - Corporate - Lic/SA

This ItemID 601854 contains an order for Microsoft Corporation VisioStd ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support

- Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

601855 Microsoft Project Standard - SAL - Corporate - Lic/SA

This ItemID 601855 contains an order for Microsoft Corporation Prjct Std ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

601856 Microsoft Visio Professional - SAL - Corporate - Lic/SA

This ItemID 601856 contains an order for Microsoft Corporation VisioPro ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)

- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

601857 Microsoft Office Professional Plus - SAL - Corporate - Lic/SA

This ItemID 601857 contains an order for Microsoft Corporation OfficeProPlus ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support

Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

601858 Microsoft Office Standard - SAL - Corporate - Lic/SA

This ItemID 601858 contains an order for Microsoft Corporation OfficeStd ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

601859 Microsoft Windows Remote Desktop Services - SAL - Corporate - Lic/SA

This ItemID 601859 contains an order for Microsoft Corporation WinRmtDsktpSrvcsSAL ALNG LicSAPk MVL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

601860 Microsoft SharePoint Server Enterprise - SAL - Corporate - Lic/SA

This ItemID 601860 contains an order for Microsoft Corporation SharePointSvr ALNG LicSAPk MVL Ent SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at

https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

601861 Microsoft SQL Server Standard - SAL - Corporate - Lic/SA

This ItemID 601861 contains an order for Microsoft Corporation SQLSvrStd ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

601862 Microsoft Exchange Server Hosted Exchange Standard - SAL - Corporate - Lic/SA

This ItemID 601862 contains an order for Microsoft Corporation ExchgStdSAL ALNG LicSAPk MVL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
    - Management of licensing key
    - Licensing provisioning support
    - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

601863 Microsoft Exchange Server Hosted Exchange Standard Plus - SAL - Corporate - Lic/SA

This ItemID 601863 contains an order for Microsoft Corporation ExchgStdPlusSAL ALNG LicSAPk MVL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
    - Management of licensing key
    - Licensing provisioning support
    - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

601864 Microsoft SQL Server Web Core (2 core pack) (minimum of 2 - 2 core packs) - Corporate - Lic/SA

This ItemID 601864 contains an order for Microsoft Corporation SQLSvrWeb ALNG LicSAPk MVL 2Lic CoreLic licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

601865 Microsoft SQL Server Enterprise Core (2 core pack) (minimum of 2 - 2 core packs) - Corporate - Lic/SA

This ItemID 601865 contains an order for Microsoft Corporation SQLSvrEntCore ALNG LicSAPk MVL 2Lic CoreLic licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit

Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

601866 Microsoft SQL Server Standard Core (2 core pack) (minimum of 2 - 2 core packs) - Corporate - Lic/SA

This ItemID 601866 contains an order for Microsoft Corporation SQLSvrStdCore ALNG LicSAPk MVL 2Lic CoreLic licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

601868 Microsoft Windows Server Standard (Core License) - 2 Core - Corporate - Lic/SA

This ItemID 601868 contains an order for Microsoft Corporation WinSvrSTDCore ALNG LicSAPk MVL 2Lic CoreLic. Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602224 Microsoft Advanced Threat Analytics - SAL - Corporate - Lic/SA

This ItemID 602224 contains an order for Microsoft Corporation AdvancedThreatAnltcsCltMgtLic ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602226 Microsoft Identity Manager - SAL - Corporate - Lic/SA

This ItemID 602226 contains an order for Microsoft Corporation IdentityMgrCAL ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.

- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602228 Microsoft Visual Studio Enterprise - SAL - Corporate - Lic/SA

This ItemID 602228 contains an order for Microsoft Corporation VSEnt ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602232 Microsoft System Center Standard (Core License) - 2 Core - Corporate - Lic/SA

This ItemID 602232 contains an order for Microsoft Corporation SysCtrStdCore ALNG LicSAPk MVL 2Lic CoreLic licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602234 Microsoft System Center Datacenter - 2 Core - Corporate - Lic/SA

This ItemID 602234 contains an order for Microsoft Corporation SysCtrDatactrCore ALNG LicSAPk MVL 2Lic CoreLic licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602236 Microsoft Core Infrastructure Server Suite Standard - 2 Core - Corporate - Lic/SA

This ItemID 602236 contains an order for Microsoft Corporation CISSteStdCore ALNG LicSAPk MVL 2Lic CoreLic licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required

- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602238 Microsoft Core Infrastructure Server Suite Datacenter - 2 Core - Corporate - Lic/SA

This ItemID 602238 contains an order for Microsoft Corporation CISSteDCCore ALNG LicSAPk MVL 2Lic CoreLic licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data

End user support

602240 Microsoft System Center Service Manager - SAL - Corporate - Lic/SA

This ItemID 602240 contains an order for Microsoft Corporation SysCtrSrvcMgrCltML ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602242 Microsoft System Center Orchestrator - SAL - Corporate - Lic/SA

This ItemID 602242 contains an order for Microsoft Corporation SysCtrOrchestratorSvr ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and

performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602244 Microsoft System Center Operations Manager - SAL - Corporate - Lic/SA

This ItemID 602244 contains an order for Microsoft Corporation SysCtrOpsMgrCltML ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602246 Microsoft System Center Data Protection Manager - SAL - Corporate - Lic/SA

This ItemID 602246 contains an order for Microsoft Corporation SysCtrDPMCltML ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602251 Microsoft Visual Studio Professional - SAL - Corporate - Lic/SA

This ItemID 602251 contains an order for Microsoft Corporation VSPro ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering

Management of licensing key
- Licensing provisioning support
- Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

https://oneneck.bigmachines.com/admin/parts/list_part_results.jsp?query=601868

602252 Microsoft Visual Studio Test Professional - SAL - Corporate - Lic/SA

This ItemID 602252 contains an order for Microsoft Corporation VSTstPro ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602253 Microsoft Azure DevOps Server Basic - SAL - Corporate - Lic/SA

This ItemID 602253 contains an order for Microsoft Corporation AzureDevOpsServer ALNG LicSAPk MVL Bsc SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602254 Microsoft Project Professional - SAL - Corporate - Lic/SA

This ItemID 602254 contains an order for Microsoft Corporation PrjctPro ALNG LicSAPk MVL SAL w1PrjctSvrSAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit

- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602256 Microsoft Skype for Business Server Standard - SAL - Corporate - Lic/SA

This ItemID 602256 contains an order for Microsoft Corporation SfBSvrStdSAL ALNG LicSAPk MVL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602259 Microsoft Skype for Business Server Enterprise - SAL - Corporate - Lic/SA

This ItemID 602259 contains an order for Microsoft Corporation SfBSrvEntSAL ALNG LicSAPk MVL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602262 Microsoft Skype for Business Server Plus - SAL - Corporate - Lic/SA

This ItemID 602262 contains an order for Microsoft Corporation SfBSvrPlusSAL ALNG LicSAPk MVL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602265 Microsoft Skype for Business Server Enterprise Plus - SAL - Corporate - Lic/SA

This ItemID 602265 contains an order for Microsoft Corporation SfBSvrEntPlusSAL ALNG LicSAPk MVL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.

- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602268 Microsoft System Center Endpoint Protection - SAL - Corporate - Lic/SA

This ItemID 602268 contains an order for Microsoft Corporation SysCtrEndpntPrtctn ALNG LicSAPk MVL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602271 Microsoft Skype for Business Server Standard for Software Assurance - SAL - Corporate - Lic/SA

This ItemID 602271 contains an order for Microsoft Corporation SfBSvrStdSAL ALNG LicSAPk MVL forSA licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602274 Microsoft Skype for Business Server Enterprise for Software Assurance - SAL - Corporate - Lic/SA

This ItemID 602274 contains an order for Microsoft Corporation SfBSrvEntSAL ALNG LicSAPk MVL forSA licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602277 Microsoft Skype for Business Server Plus for Software Assurance - SAL - Corporate - Lic/SA

This ItemID 602277 contains an order for Microsoft Corporation SfBSvrPlusSAL ALNG LicSAPk MVL forSA licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required

- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602280 Microsoft SharePoint Server Enterprise for Software Assurance - SAL - Corporate - Lic/SA

This ItemID 602280 contains an order for Microsoft Corporation SharePointSvr ALNG LicSAPk MVL Ent SAL forSA Student licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data

End user support

602283 Microsoft Exchange Server Hosted Exchange Enterprise for Software Assurance - SAL - Corporate - Lic/SA

This ItemID 602283 contains an order for Microsoft Corporation ExchgEntSAL ALNG LicSAPk MVL forSA Student licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602289 Microsoft System Center Configuration Manager - SAL - Corporate - Lic/SA

This ItemID 602289 contains an order for Microsoft Corporation SysCtrCnfgMgrCltML ALNG LicSAPk MVL SAL licensing of

software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602293 Microsoft Productivity Suite for Enterprise CAL Software Assurance - SAL - Corporate - Lic/SA

This ItemID 602293 contains an order for Microsoft Corporation ProductivitySteSAL ALNG LicSAPk MVL ForEntCALSA licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602302 Microsoft Windows Server Essentials - (Processer License) - Corporate - Lic/SA

This ItemID 602302 contains an order for Microsoft Corporation WinSvrEssntls ALNG LicSAPk MVL 1Proc licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602303 Microsoft Windows Server Active Directory Rights Management Services - SAL - Corporate - Lic/SA

This ItemID 602303 contains an order for Microsoft Corporation WinRghtsMgmtSrvcsCAL ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering

Management of licensing key
- Licensing provisioning support
- Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602305 Microsoft Exchange Server Hosted Exchange Basic - SAL - Corporate - Lic/SA

This ItemID 602305 contains an order for Microsoft Corporation ExchgBscSAL ALNG LicSAPk MVL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until

such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602307 Microsoft Exchange Server Hosted Exchange Enterprise - SAL - Corporate - Lic/SA

This ItemID 602307 contains an order for Microsoft Corporation ExchgEntSAL ALNG LicSAPk MVL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing

requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602309 Microsoft Exchange Server Hosted Exchange Enterprise Plus - SAL - Corporate - Lic/SA

This ItemID 602309 contains an order for Microsoft Corporation ExchgEntPlusSAL ALNG LicSAPk MVL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management

Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602317 Microsoft SharePoint Server Standard - SAL - Corporate - Lic/SA

This ItemID 602317 contains an order for Microsoft Corporation SharePointSvr ALNG LicSAPk MVL Std SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602319 Microsoft Project Server - SAL - Corporate - Lic/SA

This ItemID 602319 contains an order for Microsoft Corporation PrjctSvr ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602321 Microsoft SharePoint Hosting - Corporate - Lic/SA

This ItemID 602321 contains an order for Microsoft Corporation SharePointHosting ALNG LicSAPk MVL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602323 Microsoft BizTalk ServerStandard - 2 Core - Corporate - Lic/SA

This ItemID 602323 contains an order for Microsoft Corporation BztlkSvrStd ALNG LicSAPk MVL 2Lic CoreLic licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.

- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602325 Microsoft BizTalk Server Enterprise - 2 Core - Corporate - Lic/SA

This ItemID 602325 contains an order for Microsoft Corporation BztlkSvrEnt ALNG LicSAPk MVL 2Lic CoreLic licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602327 Microsoft BizTalk Server Branch - 2 Core - Corporate - Lic/SA

This ItemID 602327 contains an order for Microsoft Corporation BztlkSvrBrnch ALNG LicSAPk MVL 2Lic CoreLic licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602329 Microsoft User Experience Virtualization Hosting for Desktops - SAL - Corporate - Lic/SA

This ItemID 602329 contains an order for Microsoft Corporation UserExpVirtSAL ALNG LicSAPk MVL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602330 Microsoft Cloud Platform Suite - Per Proc - Corporate - Lic/SA

This ItemID 602330 contains an order for Microsoft Corporation CloudPltfrmSte ALNG LicSAPk MVL 1Proc licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required

- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602331 Microsoft Cloud Platform Guest - Per OSE - Corporate - Lic/SA

This ItemID 602331 contains an order for Microsoft Corporation CloudPltfrmGuest ALNG LicSAPk MVL PerOSE licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data

End user support

602332 Microsoft SharePoint Server Standard for Software Assurance - CAL - Corporate - Lic/SA

This ItemID 602332 contains an order for Microsoft Corporation SharePointStdCAL ALNG LicSAPk MVL SAL forSA licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602333 Microsoft Exchange Server Hosted Exchange Standard for Software Assurance - SAL - Corporate - Lic/SA

This ItemID 602333 contains an order for Microsoft Corporation ExchgStdSAL ALNG LicSAPk MVL forSA licensing of software (

Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602335 Microsoft Productivity Suite - SAL - Corporate - Lic/SA

This ItemID 602335 contains an order for Microsoft Corporation ProductivitySteSAL ALNG LicSAPk MVL Student licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602336 Microsoft Productivity Suite For Core CAL Suite- SAL - Corporate - Lic/SA

This ItemID 602336 contains an order for Microsoft Corporation ProductivitySteSAL ALNG LicSAPk MVL ForCoreCALSA licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602337 Microsoft Office Multi-Language Pack - SAL - Corporate - Lic/SA

This ItemID 602337 contains an order for Microsoft Corporation OfficeMultiLangPk ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering

Management of licensing key
- Licensing provisioning support
- Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

602338 Microsoft Azure DevOps Server - SAL - Corporate - Lic/SA

This ItemID 602338 contains an order for Microsoft Corporation AzureDevOpsServer ALNG LicSAPk MVL SAL licensing of software (Microsoft Offering). Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Microsoft Offering will be provided and made by Microsoft Corporation and may be subject to change as determined by Microsoft Corporation.

Client agrees that the Microsoft Offerings are subject to the then current Microsoft SPLA Volume Licensing End User License Terms available at https://www.oneneck.com/privacy-and-terms and Microsoft s privacy statement located at https://privacy.microsoft.com/en-us/privacystatement, which are hereby incorporated into this Statement of Work.

Terms

- Notwithstanding the term of this Statement of Work, this Microsoft Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Microsoft.

Company's Responsibilities and Included Features

Licensing

- Provide Microsoft Offering on a monthly subscription basis

Technical Support

- Technical support for Microsoft Offering
  - Management of licensing key
  - Licensing provisioning support
  - Provide operating system software for installation or supervised installation of application software

Service Invoicing

- Invoicing for this Service will commence at the time of provisioning of the Microsoft Offering and will continue until

such software is de-provisioned.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Adherence to Microsoft licensing requirements. For more information on Microsoft Offering specific licensing requirements, see https://www.microsoft.com/en-us/licensing/default
- All software licensing not contractually provided by Company (including other Microsoft software)
- If the software is to be installed on Client owned infrastructure, subscription to Company managed services on virtual infrastructure is required
- Provide access to Company upon request for inventory and audit
- Operating system management
- Application management
- Application functional support
- Content or data related support
- All backups, including but not limited to application and proprietary data
- End user support

Category: Licensing Other

600063 Oracle Linux Basic Support

Company's Responsibilities and Included Features

Subscription Licensing

- Provide described software licensure on a monthly subscription basis with a 1 year commitment
- Management of license key

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Commitment to a 1 year subscription
- Application management
- Application functional support
- Content or data related support
- Backups of application and proprietary data
- End user support

600064 Oracle VM Premier Limited Support

Company's Responsibilities and Included Features

Subscription Licensing

- Provide described software licensure on a monthly subscription basis with a 1 year commitment
- Management of license key

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Commitment to a 1 year subscription
- Application management
- Application functional support
- Content or data related support
- Backups of application and proprietary data
- End user support

600093 Cisco Nexus 1000V Series Switch for VMware - Subscription License

Company's Responsibilities and Included Features

Subscription Licensing

- Provide described software licensure on a monthly subscription basis
- Management of license key

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Application management
- Application functional support
- Content or data related support
- Backups of application and proprietary data
- End user support

601688 VMware Horizon Standard Edition Licensing

This ItemID 601684 contains an order for licensing of software provided by VMware, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the VMware offerings will be provided and made by VMware, Inc. and may be subject to change as determined by VMware, Inc.

Client agrees that the VMware Offerings are subject to the VMware Services End User License Agreement available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf and privacy policy located at https://www.vmware.com/help/privacy.html, which are hereby incorporated into this Statement of Work.

Definitions

Active Connection: Any connections to powered on desktop virtual machines, Remote Desktop Services sessions or physical computers.

Concurrent Users: The total number of users accessing or using the software at any given time to maintain an Active Connection, including active and idle session states, to their desktop through each endpoint device.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based VMware software licensing for VMware s Horizon Standard Edition which includes the following software only components:

- VMware Horizon (includes View Manager, View Composer and Persona Management)
- VMware ThinApp Client
- VMware ThinApp Packager
- VMware Workstation
- VMware vCenter Server Desktop
- VMware vSphere Enterprise Plus for Desktop

Service Metering

- This is a metered service.
- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by VMware.
- Usage metering for billing is calculated based on the highest total concurrent connections for a given month as viewed

in the Horizon administrator management web user interface. The count will be reset at the end of each month.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Subscription to Company VMware vSphere managed services is required
- Subscription to Company VMware Horizon Standard Edition managed services is required
- Client must relinquish primary management and administrative control of the subscribed software to Company. However, Client may elect to self-provision and self-manage some or all of the following elements:
  - VMware Horizon (includes View Manager, View Composer and Persona Management)
  - VMware ThinApp Client
  - VMware ThinApp Packager
  - VMware Workstation
  - VMware vCenter Server Desktop

601690 VMware vCloud Flex Core Bundle

This ItemID 601690 contains an order for licensing of software provided by VMware, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the VMware offerings will be provided and made by VMware, Inc. and may be subject to change as determined by VMware, Inc.

Client agrees that the VMware Offerings are subject to the VMware Services End User License Agreement available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf and privacy policy located at https://www.vmware.com/help/privacy.html, which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide monthly subscription-based VMware software licensing for VMware s vCloud Flex Core Bundle which includes the following software only components:

- Management
  - vCloud Director
  - vRealize Log Insight
- Metering/Billing
  - vRealize Operations Chargeback
  - vCloud Usage Meter
- Networking
  - NSX Data Center SP Base
- Compute
  - vSphere Enterprise Plus
  - vCenter Server Standard
- Support
  - Production Level Support

Service Metering

- This is a metered service.
- Usage metering for billing RAM is calculated for the powered on Virtual Machine (VM) by taking the greater value of:
  - 1. Reserved RAM as defined by VMware
  - 2. 50% of allocated RAM as defined by VMware
- Billed RAM is billing RAM x time in hours (i.e. as calculated by the VMware vCloud Usage Meter). The billed RAMs are summed, converted to GB and then divided by the total number of hours in the month to give the Average Billed RAM (GB).
- Once the value is taken from the two calculations above, all GB above 24 will be capped at 24GB

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month to month basis.

- Company may revise terms of use or pricing to reflect changes by VMware.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Subscription to Company VMware vSphere managed services is required
- Client must relinquish primary management and administrative control of the subscribed software to Company. However, Client may elect to self-provision some or all of the following elements through its access to vCenter for VM lifecycle management:
  - Virtual hardware management
  - Virtual network attachment
  - Virtual storage management
  - Remote console access
  - Access to shared VM templates
  - Access to private VM templates
  - Access to shared software ISO repository
  - Access to private software ISO repository
  - Snapshot management

601871 Nutanix Files License Service - AOS

Company's Responsibilities and Included Features

Nutanix Files License Service - AOS (NFLS) provides Nutanix Files software for Clusters running mixed workloads (server virtualized and Nutanix Files). NFLS is billed monthly per GiB storage space consumed basis. Nutanix Files is a software-defined scale-out file storage solution designed to address a wide range of use cases, including support for Linux and Windows home directories, user profiles and department shares.

Nutanix Files Features

- Server Message Block (SMB) versions 2 and 3 (SMBv2 and SMB v3) support
- Network File System (NFS) versions 3 and 4 (NFSv3 and NFSv4) support
- Multiprotocol support
- High availability architecture
- Self-service file restoration
- Hot workloads performance tier

Metered Service

- This service is metered
- The quantity of (NFLS) storage space is comprised of replicated stored data, file storage and snapshot space
- The quantity is measured hourly
- Usage for a month is the average of the hourly measurements captured during that month.

Terms

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Nutanix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Subscribe to Company s Managed Services for Nutanix Files Management
- Subscribe to Company s ReliaCloud EDGE Node service

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of NFLS is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.

Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

601872 Nutanix Files License Service - EDGE Files Node

Company's Responsibilities and Included Features

Nutanix Files License Service - EDGE Files Node (NFLS) provides Nutanix Files software for ReliaCloud EDGE Files node-based clusters. NFLS is billed monthly per GiB storage space consumed basis. Nutanix Files is a software-defined scale-out file storage solution designed to address a wide range of use cases, including support for Linux and Windows home directories, user profiles and department shares.

Nutanix Files Features

- Server Message Block (SMB) versions 2 and 3 (SMBv2 and SMB v3) support
- Network File System (NFS) versions 3 and 4 (NFSv3 and NFSv4) support
- Multiprotocol support
- High availability architecture
- Self-service file restoration
- Hot workloads performance tier

Metered Service

- This service is metered
- The quantity of (NFLS) storage space is comprised of replicated stored data, file storage and snapshot space
- The quantity is measured hourly
- Usage for a month is the average of the hourly measurements captured during that month.

Terms

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Nutanix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Subscribe to Company s ReliaCloud EDGE Files Node service

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of NFLS is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

601931 Veeam Backup for Microsoft Office 365 License

A detailed product description of Veeam Backup for Microsoft Office 365 is available at https://www.veeam.com/backup-microsoft-office-365.html.

Notwithstanding the term of this Statement of Work, Veeam Backup for Microsoft Office 365 License is provided on a month to month basis. Company may revise term, terms of use or pricing to reflect changes by Veeam upon thirty (30) days advance notice.

Definitions

User: A named user with Microsoft Office 365 that is backed up using the contracted Veeam Backup for Microsoft Office 365

License.

Company's Responsibilities and Included Features

Licenses

Provide Veeam Backup for Microsoft Office 365 License (Veeam Backup for O365) on a per User per month basis.

Service Metering

Provide Veeam Backup for Microsoft Office 365 License (Veeam Backup for O365) on a per User per month basis.

- This is a metered service billed in arrears on a monthly basis
- Client will be billed for the maximum number of individual Users per month

Client's Responsibilities and Out-of-Scope Notes

Unless contracted separately with Company under this or another Executed Order, Client is responsible for the following:

- Configuration and ongoing management of Veeam Backup for O365
- Providing infrastructure resources to run the Veeam Backup for O365 server(s) and proxy, if applicable
- Contracting and management of Microsoft Office 365 services
- Contract for Company ReliaCloud Object Services to act as the backup repository

End User License Agreement

Client agrees that the Service is subject to the Veeam End User License Agreement (EULA) available at https://www.veeam.com/eula.html and Client acknowledges and accepts that its subscription to and use of this Service is subject to the EULA.

603926 Oracle Linux Premier Limited Support

Company's Responsibilities and Included Features

Subscription Licensing

- Provide described software licensure on a monthly subscription basis with a 1 year commitment
- Management of license key

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Commitment to a 1 year subscription
- Application management
- Application functional support
- Content or data related support
- Backups of application and proprietary data
- End user support

603927 Oracle Linux Extended Support

Company's Responsibilities and Included Features

Subscription Licensing

- Provide described software licensure on a monthly subscription basis with a 1 year commitment
- Management of license key

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Commitment to a 1 year subscription
- Application management
- Application functional support
- Content or data related support
- Backups of application and proprietary data
- End user support

603928 Oracle VM Extended Support

Company's Responsibilities and Included Features

Subscription Licensing

- Provide described software licensure on a monthly subscription basis with a 1 year commitment
- Management of license key

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Commitment to a 1 year subscription
- Application management
- Application functional support
- Content or data related support
- Backups of application and proprietary data
- End user support

606609 Nutanix Calm Licensing Service - Per VM

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Calm: A Nutanix cloud software suite that allows you to select, provision, and manage business applications across both private and public clouds. Calm provides application life cycle, monitoring, and remediation to manage your heterogeneous infrastructure, for example, VMs, containers, and bare-metal servers. Nutanix Calm supports multiple platforms so that you can use a single self-service and automation interface to manage your infrastructure. Calm is an add-on software component to an Nutanix Cluster.

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

Nutanix Calm License Service - Per VM (Service) provides subscription access to Nutanix Calm software.

The Service is a software license only, it does not provide any hardware, other Nutanix software or Service management. Nutanix Calm software is licensed per VM. The licensing is available to all Nodes within the Cluster.

The following are the salient features of Calm:

- Application life-cycle management: Automates the provisioning and deletion of both traditional multi-tiered applications and modern distributed services by using blueprints that deploy applications in both private and public cloud.
- Customizable blueprints: The ability to create blueprints that deploy and allow the of management custom enterprise applications by incorporating the elements of each application, including relevant VMs, configurations, and related

binaries.
- Nutanix Marketplace: Publishes application blueprints directly to end users through Marketplace.
- Governance: Role-based governance limiting user operations that are based on permissions.
- Hybrid cloud management: Automates the provisioning of hybrid cloud infrastructure, scaling both multi-tiered and distributed applications across cloud environments, including Nutanix AHV, AWS, VMware (on both Nutanix and non-Nutanix platforms), Google Cloud Platform and Microsoft Azure.

Additional Calm features and product descriptions can be found at https://www.nutanix.com/products/cloud-manager/self-service

Unit of Measure:

- This service is consumed per VM in any state (on or off) while under the management of Nutanix Calm. VMs will be billed in whole hour increments, rounding up partial hour usage to the next full hour.
- Service billing is monthly

Term

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month-to-month basis.
- Company may revise terms of use or pricing to reflect changes by Nutanix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This service is a software license only:

General Requirements

- Subscribe to Company ReliaCloud EDGE Node services
- Prism Central instance must be hosted on one of the AHV clusters registered with it
- Deployment and configuration of Calm
- Management and operation of Calm
- Blueprint development, implementation and management
- Run book development, implementation and management

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix Calm is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.

- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

606611 Nutanix Files License Service - AOS Per TiB

Company's Responsibilities and Included Features

Nutanix Files License Service - AOS per TiB (NFLS) provides Nutanix Files software for Clusters running mixed workloads (server virtualized and Nutanix Files). NFLS is billed monthly per TiB of file storage space. Nutanix Files is a software-defined scale-out file storage solution designed to address a wide range of use cases, including support for Linux and Windows home directories, user profiles and department shares.

The Service is a software license only, it does not provide any hardware, other Nutanix software or Service management.

The following are the salient features of Nutanix Files:

Nutanix Files (Files) is a software-defined, scale-out file storage solution that lets you share files in a centralized and protected

location to eliminate the requirement for a third-party file server.

- Server Message Block (SMB) versions 2 and 3 (SMBv2 and SMB v3) support
- Network File System (NFS) versions 3 and 4 (NFSv3 and NFSv4) support
- AHV and ESXi hypervisor support.
- Multiprotocol support
- High availability for both VMs and data
- Load balancing through scale-up and scale-out
- Data management including Smart Tiering, Smart Sync, Smart DR, protection domain (PD) based-DR, and Self-Service Restore (SSR).

Additional Files features and product descriptions can be found at https://www.nutanix.com/products/files

Metered Service:

- This service is metered
- The quantity of (NFLS) storage space is comprised of replicated stored data, file storage and snapshot space
- The quantity of TiBs is measured hourly and billed monthly

Terms

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Nutanix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General

- Procurement of necessary hardware and other associated software to create a Nutanix Cluster
- Management of all hardware and software associated with the solution

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of NFLS is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

606612 Nutanix Objects License Service - AOS Per TiB

Company's Responsibilities and Included Features

Nutanix Objects License Service - AOS per TiB (NOLS) provides Nutanix Objects software for Clusters running mixed workloads (server virtualized and Nutanix Objects). NOLS is billed monthly per TiB of Objects storage space. Nutanix Objects is a software-defined Object store sevice storage solution designed to addresses storage-related use cases for backup, and long-term retention, and data storage for your cloud-native applications by using standard S3 APIs

The Service is a software license only, it does not provide any hardware, other Nutanix software or Service management.

The following are the salient features of Nutanix Objects:

- Write-Once-Read-Many (WORM)

Immutability
- Object Versioning
- Data Life Cycle Management
- Multipart Upload
- Data-at-Rest Encryption with Native Key Management
- Multi-protocol Access

Additional Files features and product descriptions can be found at https://www.nutanix.com/products/objects

Metered Service:

- This service is metered
- The quantity of (NOLS) storage space is comprised of Objects storage space
- The quantity of TiBs is measured hourly and billed monthly

Terms

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Nutanix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General

- Procurment of necessary hardware and other associated software to create a Nutanix Cluster
- Management of all hardware and software associated with the solution

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of NOLS is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

609701 VMware Cloud Foundation Subscription

This ItemID 609701 contains an order for a software subscription provided by Broadcom, Inc. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the VMware offerings will be provided and made by Broadcom, Inc. and may be subject to change as determined by Broadcom, Inc. Company will be the sole licensee of VMware Cloud Foundation

Client agrees that the Broadcom Offerings are subject to the VMware End User License Agreement available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf and to the privacy policy located at https://www.vmware.com/help/privacy.html, which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide a subscription-based VMware software licensing for VMware Cloud Foundation (VCF), which includes the following components and quantities per core of VCF:

- vSphere Enterprise Plus: 1 core with 16-core per CPU minimum
- vCenter Standard: 1 instance
- Tanzu Kubernetes Grid: 1 core
- vSAN Enterprise: 1 TiB of vSAN per core

- Aria Suite Enterprise: 1 core
- NSX Networking for VCF: 1 core
- HCX Enterprise: 1 core
- Aria Operations Network Enterprise: 1 core
- Data Services Manager: 1 core
- SDDC Manager: 1 core

Terms

- Notwithstanding the term of this Statement of Work, this Service is provided on a month-to-month basis and may be terminated for convenience by either party with a 30 days notice before the end of the month
- Company may revise the terms of use or pricing to reflect changes by Broadcom

Service Metering

- This is a metered service based upon the number of physical cores on servers running VCF
- All physical CPUs must be licensed on servers running VCF. A minimum of 16 cores per CPU must be licensed
- Usage over the committed quantity will be billed as overage, under ItemID 609702 VMware Cloud Foundation Subscription Overage

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Subscription to Company VMware vSphere managed services is required
- Client must relinquish primary management and administrative control of the subscribed software to Company. However, Client may elect to self-provision some or all of the following elements through its access to vCenter for VM lifecycle management:
  - Virtual hardware management
  - Virtual network attachment
  - Virtual storage management
  - Remote console access
  - Access to shared VM templates
  - Access to private VM templates
  - Access to shared software ISO repository
  - Access to private software ISO repository
  - Snapshot management

Mandatory Upgrade Regiments

- Client s environment must be on the latest major software version minus one (N-1) for no more than 6 months for new deployments, and for no more than 12 months for existing deployments. That is, once a new major VCF software version is released, Client is required to move to the latest major software version within 6 months for new deployments and within 12 months for existing deployments
- Client is required to deploy consistent software versions for all deployed components of VCF. For example, VCF software version 5.1 has components vSphere version 8 and vSAN version 8. Client is not permitted to deploy vSphere version 8 with vSAN version 7 inside a Client s VMware environment

609702 VMware Cloud Foundation Subscription Overage

VMware Cloud Foundation Subscription Overage is an add-on component to ItemID 609701 VMware Cloud Foundation Subscription

Any usage over the contracted quantity for 609701 VMware Cloud Foundation Subscription will be billed under this ItemID

611498 Nutanix Cloud Platform Software - NCI ULT/NCM PRO Bundle

Definition

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

NCI ULT: Nutanix Cloud Infrastructure Ultimate

NCM PRO: Nutanix Cloud Manager Pro

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

CPU core Core : An individual processing unit within a CPU (Central Processing Unit), responsible for executing instructions and performing calculations

Company's Responsibilities and Included Features

Definition

Nutanix Cloud Platform Software NCI Ult/NCM Pro Bundle Service provides subscription access to Nutanix Cloud Platform software on a per Core per month basis.

The Service is for Nutanix Cloud Platform software licensing only, and does not provide any hardware, other Nutanix software, or Service management. Nutanix Cloud Platform software is licensed per Core. All Cores within the Cluster must be licensed for Nutanix Cloud Platform, as such Service quantities will automatically be adjusted by Company as Core quantities are adjusted.

The following are the salient features of the bundled software:

- Nutanix AOS
- Nutanix AHV
- Nutanix Disaster Recovery
- Lifecycle Manager
- Prism Central
- Self-Service and Orchestration

Additional Files features and product descriptions can be found at https://www.nutanix.com/products/cloud-platform/software-options

Software Bundle Specifications:

Company will provide Nutanix Cloud Platform licensing that provides a sofware release that meets or exceeds the following software editions:

- Nutanix NCI (Nutanix Cloud Infrastructure) Ultimate
- Nutanix NCM (Nutanix Cloud Manager) Pro

The licensing includes the following Nutanix software that can be self-enrolled and disenrolled by Client. Usage of this software may incur additional charges as defined by the Agreement:

- Nutanix Unified Storage Pro Per TiB
- Nutanix Unified Storage Starter Per TiB

Terms

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month to month basis.
- Company may revise terms of use or pricing to reflect changes by Nutanix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This service is a software license only:

General Requirements

- Subscribe to Company Nutanix management services.
- License all Nodes within the cluster with the Service.

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix Cloud Platform software is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

,9.59,9.59,40.7,0.0%,40.7,40.7,76.44%, 279

Category: Licensing SPLA

602187 NVIDIA vWS Virtual GPU Software per Named User Service

Definitions

GPU: Graphics processing unit (GPU) is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device.

Named User License (Named Users): Is a license that may only be used by a single named authorized user and such authorized user may not re-assign or share the license with any other person (including, without limitation, other authorized users); provided, however, that if the named authorized user is no longer employed or no longer requires any access to the Cluster as part of his or her job, Client may re-assign a named user license to a new named authorized user.

vGPU: Virtual graphics processing unit.

Company's Responsibilities and Included Features

NVIDIA vWS (virtual workstation) Virtual GPU Software per Named User Service (NVIDIA vWS) provides NVIDIA virtual GPU licensing on a per named user per month basis. The NVIDIA vWS product is designed for mainstream and high-end designers who use powerful 3D content creation applications such as Dassault CATIA, SOLIDWORKS, 3DExcite, Siemens NX, PTC Creo, Schlumberger Petrel, or Autodesk Maya. NVIDIA vWS allows users to access their professional graphics applications with full features and performance from a supported services and devices.

Metered Service:

- This service is metered
- Named Users are measured from the NVIDA GPU Software License Server provided by Company.
- The quantity of Named Users is calculated on the maximum number of Named Users identified within the virtualization platform per month.

Term

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month-to-month basis.
- Company may revise terms of use or pricing to reflect changes by NVIDIA.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This service is a software license only:

General Requirements

- Open network ports within the virtualization platform to allow communication to and from the Company provided NVIDIA vGPU Software License Server.
- Allow company to install any necessary software such as drivers for the NVIDIA GPU cards
- Subscribe to Company's ReliaCloud EDGE EUC Nodes with GPUs

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of NVIDIA vWS (virtual workstation) Virtual GPU Software is NVIDIA Corporation (NVIDIA) and may be subject to changes in provisioning and performance as determined by NVIDIA.
- Client agrees that NVIDIA offerings provided herein are subject to the NVIDIA End User License Agreement for GPU available https://images.nvidia.com/content/pdf/grid/support/enterprise-eula-grid-and-amgx-supplements.pdf which is hereby incorporated into this SOW in full.

602188 NVIDIA vPC Virtual GPU Software per Named User Service

Definitions

GPU: Graphics processing unit (GPU) is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device.

Named User License (Named Users): Is a license that may only be used by a single named authorized user and such authorized user may not re-assign or share the license with any other person (including, without limitation, other authorized users); provided, however, that if the named authorized user is no longer employed or no longer requires any access to the Cluster as part of his or her job, Client may re-assign a named user license to a new named authorized user.

vGPU: Virtual graphics processing unit.

Company's Responsibilities and Included Features

NVIDIA vPC (virtual Personal Computer) Virtual GPU Software per Named User Service (NVIDIA vPC) provides NVIDIA virtual GPU licensing on a per named user per month basis. The NVIDIA vPC product is designed for an enhanced virtual desktop experience for users that leverage streaming applications, browsers and high-definition video.

Metered Service:

- This service is metered
- Named Users are measured from the NVIDA GPU Software License Server provided by Company.
- The quantity of Named Users is calculated on the maximum number of Named Users identified within the virtualization platform per month.

Term

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month-to-month basis.
- Company may revise terms of use or pricing to reflect changes by NVIDIA.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This service is a software license only:

General Requirements

- Open network ports within the virtualization platform to allow communication to and from the Company provided NVIDIA vGPU Software License Server.
- Allow company to install any necessary software such as drivers for the NVIDIA GPU cards
- Subscribe to Company's ReliaCloud EDGE EUC Nodes with GPUs

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of NVIDIA vPC Virtual GPU Software is NVIDIA Corporation (NVIDIA) and may be subject to changes in provisioning and performance as determined by NVIDIA.

- Client agrees that NVIDIA offerings provided herein are subject to the NVIDIA End User License Agreement for GPU available https://images.nvidia.com/content/pdf/grid/support/enterprise-eula-grid-and-amgx-supplements.pdf which is hereby incorporated into this SOW in full.

602356 Nutanix Frame Named User License Service

Definition

Named User License (Named User): Is a license that may only be used by a single named authorized user and such authorized user may not re-assign or share the license with any other person (including, without limitation, other authorized users); provided, however, that if the named authorized user is no longer employed or no longer requires any access to the Cluster as part of his or her job, Client may re-assign a named user license to a new named authorized user.

Company's Responsibilities and Included Features

Nutanix Frame Named User License Service ("NFLS)" provides subscription access to Nutanix Frame Frame on a per Named User per month basis. Nutanix Frame is a Desktop-as-a-Service (DaaS) solution that provides the ability to run virtual apps and desktops on your choice of infrastructure.

Frame is a control plane that runs in the cloud and is hosted and operated by Nutanix. End-user workloads are orchestrated by the Frame service and can run in a variety of public clouds and in your own private cloud with Frame on Nutanix AOS.

Metered Service:

- This service is metered
- The quantity of Named Users is calculated on the maximum number of Named Users identified within the Cluster per month.

Term

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month-to-month basis.
- Company may revise terms of use or pricing to reflect changes by Nutanix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This service is a software license only:

General Requirements

- Provide or subscribe to cloud infrastructure (hardware and virtualization software) that supports the virtual application or desktop sessions that Frame manages and instantiates.
- Provide all supporting desktop operating system and application software licensing
- Management and operation of Frame, including but not limited to; building of golden images, application installation, selection of infrastructure instances aligned to desktop or application hosting, configuration of authentication integration, report creation, VPN integration and other usage customizations.
- Management and support of end user sessions and end points (laptops, desktops, tablets, phones and other devices)
- Provide and provision end points

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of NFLS is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

602396 Nutanix Era License Service

Definitions

vCPU Virtual Central Processing Unit, also known as a virtual processor, represents or share of a physical CPU that is assigned to a virtual machine (VM).

Company's Responsibilities and Included Features

Nutanix Era License service provides a license to use Nutanix Era software on a per vCPU per month basis. This is a software only service and does not provide any level of Company management services.

Nutanix Era (Era) is a cloud agnostic multi-database managements solution for IT and database teams. Era supports Oracle, Microsoft SQL server, MySQL, MariaDB, Postgress, and SAP HAHA.

Core features include:

- Hybrid cloud database management
- Datbase provisiong
- Datbase Protection
- Database Patching
- Copy data management

Additional information is available at https://www.nutanix.com/products/era

Metered Service:

- This service is metered
- The service is charged upon the maximum number of vCPUs used by the VMs for which its database is managed by Era.

Terms:

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month-to-month basis.
- Company may revise terms of use or pricing to reflect changes by Nutanix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This service is a software license only:

- Provide or subscribe to cloud infrastructure (hardware and virtualization software) that supports the virtual application or desktop sessions that Frame manages and instantiates.
- Provide all supporting desktop operating system and application software licensing
- Management and operation of associated databases.

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of Era is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc. .
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full..

602742 Nutanix Flow Security License Service

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Nutanix Flow Security: A policy-driven security framework that inspects traffic within the data center. The framework uses a workload-centric approach instead of a network-centric approach. Therefore, it can scrutinize traffic to and from VMs no matter how their network configurations change and where they reside in the data center.

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

Nutanix Flow Security per Node License Service (Service) provides subscription access to Nutanix Flow Security software on a per Node per month basis.

The Service is only for Nutanix Flow Security software license only, it does not provide any hardware, other Nutanix software or Service management. Nutanix Flow software is licensed per Node. All Nodes within the Cluster must be licensed for Nutanix Flow Security, as such Service quantities will automatically be adjusted by Company as Node quantities are adjusted.

Metered Service:

- This service is metered
- The quantity of Nodes is calculated on the maximum number of active Nodes identified within the Cluster per month.

Term

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month-to-month basis.
- Company may revise terms of use or pricing to reflect changes by Nutanix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This service is a software license only:

General Requirements

- Subscribe to Company ReliaCloud EDGE Node services
- License all Nodes within the cluster with the Service.
- Cluster requires Nutanix AHV as the hypervisor
- Cluster must be running AHV on AOS 5.6 or later
- Prism Central instance must be hosted on one of the AHV clusters registered with it
- Deployment and configuration of Nutanix Flow Security Software
- Management and operation of Nutanix Flow Security Software

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix Flow Security is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.

- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

603357 Nutanix Frame Burstable Named User License Service

Definition

Named User License (Named User): Is a license that may only be used by a single named authorized user and such authorized user may not re-assign or share the license with any other person (including, without limitation, other authorized users); provided, however, that if the named authorized user is no longer employed or no longer requires any access to the Cluster as part of his or her job, Client may re-assign a named user license to a new named authorized user.

Company's Responsibilities and Included Features

Nutanix Frame Burstable Named User License Service ("NFBLS)" provides additional burst license capacity above the Nutanix Frame Committed Named User License Service quantity.

Consumption:

- NFBLS is a metered service
- NFBLS is burstable above the fixed allocation of Name Users, providing immediate access to additional capacity. Client will be billed for the maximum number of Named Users for the month at the burstable service rate less the total number of committed Name Users.
- Example:
  - 50 committed Named Users at $15 per user committed rate, $750
  - 7 additional Named Users at $25 per user burstable rate, $175.
  - Total NFLS bill $925

Term

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month-to-month basis.
- Company may revise terms of use or pricing to reflect changes by Nutanix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This service is a software license only:

General Requirements

- Subscribe to Nutanix Frame Committed Named User License Service
- Provide or subscribe to cloud infrastructure (hardware and virtualization software) that supports the virtual application or desktop sessions that Frame manages and instantiates.
- Provide all supporting desktop operating system and application software licensing
- Management and operation of Frame, including but not limited to; building of golden images, application installation, selection of infrastructure instances aligned to desktop or application hosting, configuration of authentication integration, report creation, VPN integration and other usage customizations.
- Management and support of end user sessions and end points (laptops, desktops, tablets, phones and other devices)
- Provide and provision end points

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of NFLS is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.

- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

606610 Nutanix Flow Security License Service - Per Node

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Nutanix Flow Security: A policy-driven security framework that inspects traffic within the data center. The framework uses a workload-centric approach instead of a network-centric approach. Therefore, it can scrutinize traffic to and from VMs no matter how their network configurations change and where they reside in the data center.

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

Nutanix Flow Security per Node License Service (Service) provides subscription access to Nutanix Flow Security software on a per Node per month basis.

The Service is only for Nutanix Flow Security software license only, it does not provide any hardware, other Nutanix software or Service management. Nutanix Flow software is licensed per Node. All Nodes within the Cluster must be licensed for Nutanix Flow Security, as such Service quantities will automatically be adjusted by Company as Node quantities are adjusted.

Metered Service:

- This service is metered
- The quantity of Nodes is calculated on the maximum number of active Nodes identified within the Cluster per month.

Term

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month-to-month basis.
- Company may revise terms of use or pricing to reflect changes by Nutanix.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This service is a software license only:

General Requirements

- Subscribe to Company ReliaCloud EDGE Node services
- License all Nodes within the cluster with the Service.
- Cluster requires Nutanix AHV as the hypervisor

Cluster must be running AHV on AOS 5.6 or later
- Prism Central instance must be hosted on one of the AHV clusters registered with it
- Deployment and configuration of Nutanix Flow Security Software
- Management and operation of Nutanix Flow Security Software

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix Flow Security is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

611706 NVIDIA vPC Virtual GPU Software per Concurrent User Service

Definitions

GPU: Graphics processing unit (GPU) is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device.

Concurrent User License (Concurrent User): A method of allocating licenses based on the number of VMs that are concurrently being used. A Concurrent User license allows only one concurrent VM to be hosted per license. For application streaming or session-based solutions, each concurrent user requires a Concurrent User license.

vGPU: Virtual graphics processing unit.

Company's Responsibilities and Included Features

NVIDIA vPC (virtual Personal Computer) Virtual GPU Software per Concurrent User Service (NVIDIA vPC) provides NVIDIA virtual GPU licensing on a per concurrent user per month basis. The NVIDIA vPC product is designed for an enhanced virtual desktop experience for users that leverage streaming applications, browsers and high-definition video.

Term

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month-to-month basis.
- Company may revise terms of use or pricing to reflect changes by NVIDIA.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This service is a software license only:

General Requirements

- Open network ports within the virtualization platform to allow communication to and from the Company provided NVIDIA vGPU Software License Server.
- Allow company to install any necessary software such as drivers for the NVIDIA GPU cards
- Subscribe to Company's ReliaCloud EDGE EUC Nodes with GPUs

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of NVIDIA vPC Virtual GPU Software is NVIDIA Corporation (NVIDIA) and may be subject to changes in provisioning and performance as determined by NVIDIA.
- Client agrees that NVIDIA offerings provided herein are subject to the NVIDIA End User License Agreement for GPU available https://images.nvidia.com/content/pdf/grid/support/enterprise-eula-grid-and-amgx-supplements.pdf which is hereby incorporated into this SOW in full.

611707 NVIDIA vWS Virtual GPU Software per Concurrent User Service

Definitions

GPU: Graphics processing unit (GPU) is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device.

Concurrent User License (Concurrent User): A method of allocating licenses based on the number of VMs that are concurrently being used. A Concurrent User license allows only one concurrent VM to be hosted per license. For application streaming or session-based solutions, each concurrent user requires a Concurrent User license.

vGPU: Virtual graphics processing unit.

Company's Responsibilities and Included Features

NVIDIA vWS (virtual workstation) Virtual GPU Software per Concurrent User Service (NVIDIA vWS) provides NVIDIA virtual GPU licensing on a per concurrent user per month basis. The NVIDIA vWS product is designed for mainstream and high-end designers who use powerful 3D content creation applications such as Dassault CATIA, SOLIDWORKS, 3DExcite, Siemens NX, PTC Creo, Schlumberger Petrel, or Autodesk Maya. NVIDIA vWS allows users to access their professional graphics applications with full features and performance from a supported services and devices.

Term

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month-to-month basis.
- Company may revise terms of use or pricing to reflect changes by NVIDIA.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

This service is a software license only:

General Requirements

- Open network ports within the virtualization platform to allow communication to and from the Company provided NVIDIA vGPU Software License Server.
- Allow company to install any necessary software such as drivers for the NVIDIA GPU cards
- Subscribe to Company's ReliaCloud EDGE EUC Nodes with GPUs

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of NVIDIA vWS (virtual workstation) Virtual GPU Software is NVIDIA Corporation (NVIDIA) and may be subject to changes in provisioning and performance as determined by NVIDIA.

- Client agrees that NVIDIA offerings provided herein are subject to the NVIDIA End User License Agreement for GPU available https://images.nvidia.com/content/pdf/grid/support/enterprise-eula-grid-and-amgx-supplements.pdf which is hereby incorporated into this SOW in full.

Category: Load Balancing

601770 Managed A10 vThunder ADC Virtual Appliance HA 25

The Managed A10 vThunder ADC (Application Delivery Controller) Virtual Appliance (vThunder ADC) - HA (high availability) service is a combination of Company-managed services for a virtual load balancer and A10 software licensing for the purpose of running two (2) vThunder ADCs in a high availability configuration on virtualized infrastructure provided by Client or contracted to be provided by Company.

Feature Specifications

The following provides the vThunder ADC feature specifications that Company will manage:

Load Balancing Sizing

- vThunder ADC load balancer with 25 Mbps (megabits per second) protected throughput
- Maximum throughput scalable with additional Company ItemIDs to 10,000 Mbps

Application Delivery

- Comprehensive IPv4/IPv6 support
- Advanced Layer 4/Layer 7 server load balancing
- Comprehensive load balancing methods:
  - Round Robin (RR)
  - Least Connections (LC)
  - Weighted RR
  - Weighted LC
  - Fastest response
- Client-provided scriptable health check support using:
  - TCL (Tool Command Language)
  - Python
  - Perl
  - Bash
- Health checks leveraging HTTP GET and standard TCP ports

Application Security

- Secure Sockets Layer ("SSL") offload support:
  - SSL termination, SSL bridging
  - SSL proxy
  - SSL session ID reuse
- AAM (Application Access Management) integration support:
  - SAML (Security Assertion Markup Language)
  - Kerberos
  - NTLM (New Technology LAN Manager)
  - TDS (Tabular Data Stream) SQL logon
  - LDAP (Lightweight Directory Access Protocol)
  - RADIUS (Remote Authentication Dial-In User Service)
  - HTML form-based
- Comprehensive SSL/TLS (Transport Layer Security) usage support including:
  - TLS 1.2 and TLS 1.3 support comprehensive SSL/TLS support
  - TLS 1.2 and TLS 1.3 support
  - PFS (Perfect Forward Secrecy) with ECDHE (Elliptic Curve Diffie-Hellman Exchange) and other ECC (Elliptic Curve Cryptography) ciphers
  - AES-NI (Advanced Encryption Standard New Instructions) and GCM (Galois/Counter Mode) ciphers
  - Dynamically add IPs to black-white lists

Company's Responsibilities and Included Features

Load Balancer Management

- Configuration of application load balancing per Client s specifications
- Configuration of health checks if required (jointly determined by Company and Client)
- Configuration for SSL
- Integration with AAM
- SSL/TLS configuration and support
- Configuration management and backup
- Configuration and management of HA settings

- Configuration of VThunder ADCs
- System throughput and capacity management

Appliance Monitoring

- vThunder ADC up/down status
- HA failure/sync issues
- Critical vThunder ADC alerts
- Virtual IP up/down
- vPool up/down

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review of same-version patch analysis
- Application of updates and patches during Client-approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the vThunder ADC software (including major upgrades) will be conducted at Company s discretion and in accordance with industry-best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up-to-date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time-and-materials basis for such catch-up services. Client acknowledges and accepts all risk relating to its failure to provide maintenance windows for upgrades or patches.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

End of Support

The vThunder ADC is subject to an EOS Date, as described above in this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide virtualizing resources to meet or exceed the the vThunder ADC infrastructure specifications.
    - Minimum virtualized resources necessary to run the vThunder ADC are as follows:
    - Per vThunder ADC
        - 1 vCPU
        - 16 GB memory *
        - 20 GB storage
        - 2 Ethernet Interfaces (3 or more are recommended)
    - Minimum of two (2) vThunder ADCs need to be deployed for HA.
- Provide and configure desired internal and external network services
- Provide scripted health checks, if applicable, to load balancing solution

Open any necessary ports and conduits between the Appliance and Company s management services

- Specify the amount of throughput in Mbps needed to serve their applications and size the environment accordingly. Note other ItemIDs from Company may be necessary.

End User License Agreement

Client agrees that the A10 vThunder ADC, and therefore Client s use of this Service as pertains to that software is subject to the A10 End User License Agreement available at: https://www.a10networks.com/company/legal/eula/.

601771 Managed A10 vThunder ADC Virtual Appliance HA 50

The Managed A10 vThunder ADC (Application Delivery Controller) Virtual Appliance (vThunder ADC) - HA (high availability) service is a combination of Company-managed services for a virtual load balancer and A10 software licensing for the purpose of running two (2) vThunder ADCs in a high availability configuration on virtualized infrastructure provided by Client or contracted to be provided by Company.

Feature Specifications

The following provides the vThunder ADC feature specifications that Company will manage:

Load Balancing Sizing

- vThunder ADC load balancer with 50 Mbps (megabits per second) protected throughput
- Maximum throughput scalable with additional Company ItemIDs to 10,000 Mbps

Application Delivery

- Comprehensive IPv4/IPv6 support
- Advanced Layer 4/Layer 7 server load balancing
- Comprehensive load balancing methods:
  - Round Robin (RR)
  - Least Connections (LC)
  - Weighted RR
  - Weighted LC
  - Fastest response
- Client-provided scriptable health check support using:
  - TCL (Tool Command Language)
  - Python
  - Perl
  - Bash
- Health checks leveraging HTTP GET and standard TCP ports

Application Security

- Secure Sockets Layer ("SSL") offload support:
  - SSL termination, SSL bridging
  - SSL proxy
  - SSL session ID reuse
- AAM (Application Access Management) integration support:
  - SAML (Security Assertion Markup Language)
  - Kerberos
  - NTLM (New Technology LAN Manager)
  - TDS (Tabular Data Stream) SQL logon
  - LDAP (Lightweight Directory Access Protocol)
  - RADIUS (Remote Authentication Dial-In User Service)
  - HTML form-based
- Comprehensive SSL/TLS (Transport Layer Security) usage support including:

TLS 1.2 and TLS 1.3 support comprehensive SSL/TLS support
- TLS 1.2 and TLS 1.3 support
- PFS (Perfect Forward Secrecy) with ECDHE (Elliptic Curve Diffie-Hellman Exchange) and other ECC (Elliptic Curve Cryptography) ciphers
- AES-NI (Advanced Encryption Standard New Instructions) and GCM (Galois/Counter Mode) ciphers
- Dynamically add IPs to black-white lists

Company's Responsibilities and Included Features

Load Balancer Management

- Configuration of application load balancing per Client s specifications
- Configuration of health checks if required (jointly determined by Company and Client)
- Configuration for SSL
- Integration with AAM
- SSL/TLS configuration and support
- Configuration management and backup
- Configuration and management of HA settings
- Configuration of VThunder ADCs
- System throughput and capacity management

Appliance Monitoring

- vThunder ADC up/down status
- HA failure/sync issues
- Critical vThunder ADC alerts
- Virtual IP up/down
- vPool up/down

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review of same-version patch analysis
- Application of updates and patches during Client-approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the vThunder ADC software (including major upgrades) will be conducted at Company s discretion and in accordance with industry-best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up-to-date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time-and-materials basis for such catch-up services. Client acknowledges and accepts all risk relating to its failure to provide maintenance windows for upgrades or patches.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

End of Support

The vThunder ADC is subject to an EOS Date, as described above in this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide virtualizing resources to meet or exceed the the vThunder ADC infrastructure specifications.
  - Minimum virtualized resources necessary to run the vThunder ADC are as follows:
  - Per vThunder ADC
    - 1 vCPU
    - 16 GB memory *
    - 20 GB storage
    - 2 Ethernet Interfaces (3 or more are recommended)
  - Minimum of two (2) vThunder ADCs need to be deployed for HA.:
- Provide and configure desired internal and external network services
- Provide scripted health checks, if applicable, to load balancing solution
- Open any necessary ports and conduits between the Appliance and Company s management services
- Specify the amount of throughput in Mbps needed to serve their applications and size the environment accordingly. Note other ItemIDs from Company may be necessary.

End User License Agreement

Client agrees that the A10 vThunder ADC, and therefore Client s use of this Service as pertains to that software is subject to the A10 End User License Agreement available at: https://www.a10networks.com/company/legal/eula/.

601772 Managed A10 vThunder ADC Virtual Appliance HA 100

The Managed A10 vThunder ADC (Application Delivery Controller) Virtual Appliance (vThunder ADC) - HA (high availability) service is a combination of Company-managed services for a virtual load balancer and A10 software licensing for the purpose of running two (2) vThunder ADCs in a high availability configuration on virtualized infrastructure provided by Client or contracted to be provided by Company.

Feature Specifications

The following provides the vThunder ADC feature specifications that Company will manage:

Load Balancing Sizing

- vThunder ADC load balancer with 100 Mbps (megabits per second) protected throughput
- Maximum throughput scalable with additional Company ItemIDs to 10,000 Mbps

Application Delivery

- Comprehensive IPv4/IPv6 support
- Advanced Layer 4/Layer 7 server load balancing
- Comprehensive load balancing methods:
  - Round Robin (RR)
  - Least Connections (LC)
  - Weighted RR
  - Weighted LC
  - Fastest response
- Client-provided scriptable health check support using:
  - TCL (Tool Command Language)
  - Python
  - Perl
  - Bash

Health checks leveraging HTTP GET and standard TCP ports

Application Security

- Secure Sockets Layer ("SSL") offload support:
  - SSL termination, SSL bridging
  - SSL proxy
  - SSL session ID reuse
- AAM (Application Access Management) integration support:
  - SAML (Security Assertion Markup Language)
  - Kerberos
  - NTLM (New Technology LAN Manager)
  - TDS (Tabular Data Stream) SQL logon
  - LDAP (Lightweight Directory Access Protocol)
  - RADIUS (Remote Authentication Dial-In User Service)
  - HTML form-based
- Comprehensive SSL/TLS (Transport Layer Security) usage support including:
  - TLS 1.2 and TLS 1.3 support comprehensive SSL/TLS support
  - TLS 1.2 and TLS 1.3 support
  - PFS (Perfect Forward Secrecy) with ECDHE (Elliptic Curve Diffie-Hellman Exchange) and other ECC (Elliptic Curve Cryptography) ciphers
  - AES-NI (Advanced Encryption Standard New Instructions) and GCM (Galois/Counter Mode) ciphers
  - Dynamically add IPs to black-white lists

Company's Responsibilities and Included Features

Load Balancer Management

- Configuration of application load balancing per Client s specifications
- Configuration of health checks if required (jointly determined by Company and Client)
- Configuration for SSL
- Integration with AAM
- SSL/TLS configuration and support
- Configuration management and backup
- Configuration and management of HA settings
- Configuration of VThunder ADCs
- System throughput and capacity management

Appliance Monitoring

- vThunder ADC up/down status
- HA failure/sync issues
- Critical vThunder ADC alerts
- Virtual IP up/down
- vPool up/down

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review of same-version patch analysis
- Application of updates and patches during Client-approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the vThunder ADC software (including major upgrades) will be conducted at Company s discretion and in accordance with industry-best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against

Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up-to-date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time-and-materials basis for such catch-up services. Client acknowledges and accepts all risk relating to its failure to provide maintenance windows for upgrades or patches.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

End of Support

The vThunder ADC is subject to an EOS Date, as described above in this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide virtualizing resources to meet or exceed the the vThunder ADC infrastructure specifications.
  - Minimum virtualized resources necessary to run the vThunder ADC are as follows:
  - Per vThunder ADC
    - 1 vCPU
    - 16 GB memory *
    - 20 GB storage
    - 2 Ethernet Interfaces (3 or more are recommended)
  - Minimum of two (2) vThunder ADCs need to be deployed for HA.:
- Provide and configure desired internal and external network services
- Provide scripted health checks, if applicable, to load balancing solution
- Open any necessary ports and conduits between the Appliance and Company s management services
- Specify the amount of throughput in Mbps needed to serve their applications and size the environment accordingly. Note other ItemIDs from Company may be necessary.

End User License Agreement

Client agrees that the A10 vThunder ADC, and therefore Client s use of this Service as pertains to that software is subject to the A10 End User License Agreement available at: https://www.a10networks.com/company/legal/eula/.

601773 Managed A10 vThunder ADC Virtual Appliance HA 250

The Managed A10 vThunder ADC (Application Delivery Controller) Virtual Appliance (vThunder ADC) - HA (high availability) service is a combination of Company-managed services for a virtual load balancer and A10 software licensing for the purpose of running two (2) vThunder ADCs in a high availability configuration on virtualized infrastructure provided by Client or contracted to be provided by Company.

Feature Specifications

The following provides the vThunder ADC feature specifications that Company will manage:

Load Balancing Sizing

- vThunder ADC load balancer with 250 Mbps (megabits per second) protected throughput

- Maximum throughput scalable with additional Company ItemIDs to 10,000 Mbps

Application Delivery

- Comprehensive IPv4/IPv6 support
- Advanced Layer 4/Layer 7 server load balancing
- Comprehensive load balancing methods:
  - Round Robin (RR)
  - Least Connections (LC)
  - Weighted RR
  - Weighted LC
  - Fastest response
- Client-provided scriptable health check support using:
  - TCL (Tool Command Language)
  - Python
  - Perl
  - Bash
- Health checks leveraging HTTP GET and standard TCP ports

Application Security

- Secure Sockets Layer ("SSL") offload support:
  - SSL termination, SSL bridging
  - SSL proxy
  - SSL session ID reuse
- AAM (Application Access Management) integration support:
  - SAML (Security Assertion Markup Language)
  - Kerberos
  - NTLM (New Technology LAN Manager)
  - TDS (Tabular Data Stream) SQL logon
  - LDAP (Lightweight Directory Access Protocol)
  - RADIUS (Remote Authentication Dial-In User Service)
  - HTML form-based
- Comprehensive SSL/TLS (Transport Layer Security) usage support including:
  - TLS 1.2 and TLS 1.3 support comprehensive SSL/TLS support
  - TLS 1.2 and TLS 1.3 support
  - PFS (Perfect Forward Secrecy) with ECDHE (Elliptic Curve Diffie-Hellman Exchange) and other ECC (Elliptic Curve Cryptography) ciphers
  - AES-NI (Advanced Encryption Standard New Instructions) and GCM (Galois/Counter Mode) ciphers
  - Dynamically add IPs to black-white lists

Company's Responsibilities and Included Features

Load Balancer Management

- Configuration of application load balancing per Client s specifications
- Configuration of health checks if required (jointly determined by Company and Client)
- Configuration for SSL
- Integration with AAM
- SSL/TLS configuration and support
- Configuration management and backup
- Configuration and management of HA settings
- Configuration of VThunder ADCs
- System throughput and capacity management

Appliance Monitoring

- vThunder ADC up/down status
- HA failure/sync issues
- Critical vThunder ADC alerts
- Virtual IP up/down
- vPool up/down

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review of same-version patch analysis
- Application of updates and patches during Client-approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the vThunder ADC software (including major upgrades) will be conducted at Company s discretion and in accordance with industry-best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up-to-date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time-and-materials basis for such catch-up services. Client acknowledges and accepts all risk relating to its failure to provide maintenance windows for upgrades or patches.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

End of Support

The vThunder ADC is subject to an EOS Date, as described above in this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide virtualizing resources to meet or exceed the the vThunder ADC infrastructure specifications.
    - Minimum virtualized resources necessary to run the vThunder ADC are as follows:
    - Per vThunder ADC
        - 1 vCPU
        - 16 GB memory *
        - 20 GB storage
        - 2 Ethernet Interfaces (3 or more are recommended)
    - Minimum of two (2) vThunder ADCs need to be deployed for HA.:
- Provide and configure desired internal and external network services
- Provide scripted health checks, if applicable, to load balancing solution
- Open any necessary ports and conduits between the Appliance and Company s management services
- Specify the amount of throughput in Mbps needed to serve their applications and size the environment accordingly. Note other ItemIDs from Company may be necessary.

End User License Agreement

Client agrees that the A10 vThunder ADC, and therefore Client s use of this Service as pertains to that software is subject to the A10 End User License Agreement available at: https://www.a10networks.com/company/legal/eula/.

601774 Managed A10 vThunder ADC Virtual Appliance HA 500

The Managed A10 vThunder ADC (Application Delivery Controller) Virtual Appliance (vThunder ADC) - HA (high availability) service is a combination of Company-managed services for a virtual load balancer and A10 software licensing for the purpose of running two (2) vThunder ADCs in a high availability configuration on virtualized infrastructure provided by Client or contracted to be provided by Company.

Feature Specifications

The following provides the vThunder ADC feature specifications that Company will manage:

Load Balancing Sizing

- vThunder ADC load balancer with 500 Mbps (megabits per second) protected throughput
- Maximum throughput scalable with additional Company ItemIDs to 10,000 Mbps

Application Delivery

- Comprehensive IPv4/IPv6 support
- Advanced Layer 4/Layer 7 server load balancing
- Comprehensive load balancing methods:
  - Round Robin (RR)
  - Least Connections (LC)
  - Weighted RR
  - Weighted LC
  - Fastest response
- Client-provided scriptable health check support using:
  - TCL (Tool Command Language)
  - Python
  - Perl
  - Bash
- Health checks leveraging HTTP GET and standard TCP ports

Application Security

- Secure Sockets Layer ("SSL") offload support:
  - SSL termination, SSL bridging
  - SSL proxy
  - SSL session ID reuse
- AAM (Application Access Management) integration support:
  - SAML (Security Assertion Markup Language)
  - Kerberos
  - NTLM (New Technology LAN Manager)
  - TDS (Tabular Data Stream) SQL logon
  - LDAP (Lightweight Directory Access Protocol)
  - RADIUS (Remote Authentication Dial-In User Service)
  - HTML form-based
- Comprehensive SSL/TLS (Transport Layer Security) usage support including:
  - TLS 1.2 and TLS 1.3 support comprehensive SSL/TLS support
  - TLS 1.2 and TLS 1.3 support
  - PFS (Perfect Forward Secrecy) with ECDHE (Elliptic Curve Diffie-Hellman Exchange) and other ECC (Elliptic Curve Cryptography) ciphers
  - AES-NI (Advanced Encryption Standard New Instructions) and GCM (Galois/Counter Mode) ciphers
  - Dynamically add IPs to black-white lists

Company's Responsibilities and Included Features

Load Balancer Management

- Configuration of application load balancing per Client s specifications
- Configuration of health checks if required (jointly determined by Company and Client)
- Configuration for SSL
- Integration with AAM
- SSL/TLS configuration and support
- Configuration management and backup
- Configuration and management of HA settings
- Configuration of VThunder ADCs
- System throughput and capacity management

Appliance Monitoring

- vThunder ADC up/down status
- HA failure/sync issues
- Critical vThunder ADC alerts
- Virtual IP up/down
- vPool up/down

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review of same-version patch analysis
- Application of updates and patches during Client-approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the vThunder ADC software (including major upgrades) will be conducted at Company s discretion and in accordance with industry-best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up-to-date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time-and-materials basis for such catch-up services. Client acknowledges and accepts all risk relating to its failure to provide maintenance windows for upgrades or patches.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

End of Support

The vThunder ADC is subject to an EOS Date, as described above in this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide virtualizing resources to meet or exceed the the vThunder ADC infrastructure specifications.
    - Minimum virtualized resources necessary to run the vThunder ADC are as follows:
    - Per vThunder ADC
        - 1 vCPU
        - 16 GB memory *
        - 20 GB storage
        - 2 Ethernet Interfaces (3 or more are recommended)
    - Minimum of two (2) vThunder ADCs need to be deployed for HA.:
- Provide and configure desired internal and external network services
- Provide scripted health checks, if applicable, to load balancing solution
- Open any necessary ports and conduits between the Appliance and Company s management services
- Specify the amount of throughput in Mbps needed to serve their applications and size the environment accordingly. Note other ItemIDs from Company may be necessary.

End User License Agreement

Client agrees that the A10 vThunder ADC, and therefore Client s use of this Service as pertains to that software is subject to the A10 End User License Agreement available at: https://www.a10networks.com/company/legal/eula/.

Category: Managed Applications

600386 SMTP Relay Service

Company's Responsibilities and Included Features

Provide a non-redundant Simple Mail Transport Protocol (SMTP) relay service.

Limited to:

- 300 email recipients in a single email
- 100,000 emails per month
- Maximum individual message size of 50MB, including attachments.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

600387 POP/IMAP Mail Service

Company's Responsibilities and Included Features

Provide a POP/IMAP mailbox service with the following features:

- Webmail client and IMAP configuration
- 1GB of mailbox storage
- 5 email aliases
- Individual mail message size cannot be greater than 50MB including attachments
- Mail limited to 300 recipients per individual email
- Not more than 5 emails per second

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

607104 GoSecure Email Security

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Terms

Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the GoSecure offerings will be made and provided by GoSecure, Inc., and may be subject to change as determined by GoSecure, Inc. Company may revise terms of use or pricing at any time to reflect GoSecure s updates to its terms or pricing.

End User License Agreement

Client agrees that the GoSecure offerings are subject to GoSecure s Subscription Services Agreement, End User License Agreement and Service Level Agreement available at https://www.gosecure.ai/wp-content/uploads/GoSecure_AUP.pdf , https://www.gosecure.ai/wp-content/uploads/GoSecure_EULA.pdf and https://www.gosecure.ai/wp-content/uploads/GoSecure_SLA.pdf, which are hereby incorporated into this Statement of Work.

Category: Managed Dedicated Hardware

500065 Dedicated Blade Cisco UCS B200 M3 - 256GB

Company's Responsibilities and Included Features

The ReliaCloud dedicated blade service delivers a dedicated server blade solution to the Client with a fixed configuration of system resources. The dedicated blade model is designed to support a single operating system environment, verses a multiple operating system environment such as VMware.

- Provide access to a dedicated (not shared with another Client blade)
- 2 Socket, 10 Cores of At least 3.0 Ghz (60 Ghz total processor power)
- 256 Gb RAM
- Requires SAN services for Storage. Storage services (LUNs) are directly mapped via 8 GBPs fiber channel to the storage array. LUNs are not shared or accessible by other Clients.
- Requires Managed O/S by Company
- Basic setup of Blade configuration and load specified operating system
- The blades leverage an N+1 style model across the chassis
- 24/7 expert-to-expert engineering support
- Infrastructure maintenance and support
- Notify Client of any detected host level issues
- Maintain Blade Profile
- Provide administrative O/S account(login) to Client

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide O/S and Application Licenses
- Install application software and data

600227 NetApp DS2246-R5 expansion shelf

Company's Responsibilities and Included Features

Bill of Material for hardware leased as per terms of the Arrow Assignment Agreement

Ln # Qty Part Number Description

1 2 DS2246-R5 DS2246-R5

2 4 X800-42U-R6 Power Cable,In-Cabinet,C13-C14

3 2 DS2246-10.8TB-QS-R5 DSK SHLF,12x900GB,6G,QS

4 216 OS-ONTAP1-CAP2-0P-QS OS Enable,Per-0.1TB,ONTAP,Perf-Stor,0P,QS

5 2 X-02659-00 Rail Kit4-PostRnd/Sq-HoleAdj24-32

6 4 X6557-R6 Cable,SAS Cntlr-Shelf/Shelf-Shelf/HA,0.5m

7 4 X6560-R6 Cable,Ethernet,0.5m RJ45 CAT6

8 2 CS-O2-4HR-VA SupportEdge Premium 4hr Onsite,VA

9 6 X306A-R5 Disk Drive,2.0TB 7.2k,DS424x,2554/2240-4

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

None

600269 Dedicated Backup Server

Company's Responsibilities and Included Features

- Provide a Client dedicated backup server with the following specifications:
  - Rack server
  - Dual CPU
  - 64GB RAM
  - Dual Power supply
  - Quad-Port Fibre Channel HBA
  - Dual 600GB hard drive

Provide rack space, power and cooling for server. Provide Ethernet to Client hosted LAN. Provide fiber channel connectivity to SAN. Windows Server 2012 licensing. Windows Server Management.

- Antivirus management of file systems and operating system.
- Installation of a managed Antivirus console.
- Application of updates and patches to the antivirus software on server platforms only.
- Configuration and validation of virus protection and scanning on server platforms only.
- Administration of 'built-in' OS components that are bundled with the OS:
  - Performance Monitor.
  - Teaming Software.
  - Device Manager.
  - DHCP.
  - DNS.
  - WINS.

Excluding:

- Terminal Services.
- Licensing/Terminal Server Gateway.
- Windows SharePoint Services (WSS).
- Active Directory Services/ADAM/ADFS.
- Server Virtualization Services.
- Application Server(s) -IIS/WWW-IIS/FTP-IIS/SMTP.
- Certificate Services.
- Certificate Authority.
- Distributed file system.
- FS Management/DFS Replication Services.

Procurement of virus protection software and licensing for current version of virus protection system. Providing software media for installation, maintenance and configuration of the software. Procurement of current software maintenance where applicable. Installation of monitoring agents where applicable. Configuration of monitoring thresholds and parameters. Monitoring and reporting of key metrics including:

- Disk utilization.
- Processor load.
- Memory usage.

Periodic review of Microsoft operating system updates. (critical/important/security) Change notice submission, approval and application of updates.

Periodic next version analysis and recommendations. Upgrades to a new major version of the operating system or embedded OS application will be provided on time and material project basis.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

600316 MDS 9148S 16G FC switch, w/ 12 active ports

Company's Responsibilities and Included Features

Provide a Cisco CMDS 9148S 16G FC switch on a monthly subscription basis.

Bill of Materials

Ln#	Qty	Part #	Description
1	1	DS-C9148S-12PK9	MDS 9148S 16G FC switch, w/ 12 active ports
2	1	CON-SNT-C48S	SNTC-8X5XNBD MDS 9148S 16G FC switch
3	1	M9148S-PL12	MDS 9148S 16G FC 12-port upgrade license
4	16	DS-SFP-FC8G-SW	8 Gbps Fibre Channel SW SFP+, LC
5	1	DS-9148S-KIT-CSCO	MDS 9148S Accessory Kit for Cisco
6	2	CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America
7	1	M91S5K9-8.1.1	MDS 9100 Supervisor/Fabric-5, NX-OS Software Release 8.1(1)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

None

600421 Additional Cisco and NetApp Hardware as a Service

Company's Responsibilities and Included Features

Bill of Material for hardware leased as per terms of the Arrow Assignment Agreement.		
Qty	Part Number	Description
NetApp		
12	X306A-R5	Disk Drive,2.0TB 7.2k,DS424x,2554/2240-4
2	DS2246-R5	DS2246-R5
4	X6557-R6	Cable,SAS Cntlr-Shelf/Shelf-Shelf/HA,0.5m
4	X6560-R6	Cable,Ethernet,0.5m RJ45 CAT6
4	X800-42U-R6	Power Cable,In-Cabinet,C13-C14
2	DS2246-21.6TB-QS-R5	DSK SHLF,24x900GB,6G,QS
432	OS-ONTAP1-CAP2-0P-QS	OS Enable,Per-0.1TB,ONTAP,Perf-Stor,0P,QS
2	X-02659-00	Rail Kit,4-Post,Rnd/Sq-Hole,Adj,24-32
2	CS-O2-4HR-VA	SupportEdge Premium 4hr Onsite,VA
2	CS-INSTALL	BASE INSTALLATION
Cisco		
2	UCSC-C460-M4	UCS C460 M4 base chassis w/o CPU/DIMM/HDD
8	CON-OSP-C460M4	48 Months SNTC-24X7X4OS UCS C460 M4 Server,SMARTnet Onsite Premium
8	UCS-CPU-E78890E	2.2 GHz E7-8890 v4/165W 24C/60M Cache/DDR4 1866MHz
96	UCS-MR-1X322RU-G	32 GB DDR4-2133/2400-MHz RDIMM/2R/x4/1.2v 1.2 2
2	UCSC-PCIE-RSR-05	Riser card with 5 PCIe slots
16	UCSC-MRBD2-12	UCS C460 M4 DDR4 Memory Riser with 12 DIMM slots
24	UCS-HD12TB10K12G	1.2 TB 12G SAS 10K RPM SFF HDD
8	UCSC-PSU2V2-1400W	1400W V2 AC Power Supply (200 - 240V) 2U & 4U C Series
8	CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length
2	UCSC-CMA-4U	Cable Management Arm for UCS C460 M4
2	CIMC-LATEST	IMC SW (Recommended) latest release for C-Series Servers.
8	UCSC-HS-01-EX	CPU Heat Sink for UCS C460 M4 Rack Server
2	UCSC-BRCKT2-C460	Bracket and Supercap cable for C460 M4 and 12 drive RAID
2	UCS-M4-V4-LBL	Cisco M4 - v4 CPU asset tab ID label (Auto-Expand)
2	UCSC-PCIE-FLR-F	Full Height PCIe slot filler for C Series
2	UCSC-RAIL-4U	Rail Kit for UCS C460 M4
2	UCSC-PCIE-RSR-FLR	PCIe Module Filler Panel for UCS C460 M4

2	UCSC-MRAID12G-4GB	Cisco 12Gbps SAS 4GB FBWC Cache module (Raid 0/1/5/6)
2	UCSC-MRAIDC460	Cisco 12G SAS Modular Raid Controller (12 port)
4	UCSC-PCIE-E16002	Emulex LPe16002 Dual-Port 16Gb Fibre Channel HBA w/SR Optics
4	UCSC-PCIE-CSC-02	Cisco VIC 1225 Dual Port 10Gb SFP+ CNA
2	C1UCS-OPT-OUT	Cisco ONE Data Center Compute Opt Out Option

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

None

600423 Cisco BE6K, PoE switches, phones, gateway for managed VoIP system

Company's Responsibilities and Included Features

Bill of Material for Hardware as a Service		
Qty	Part Number	Description
1	CON-SNTP-BE6M4M4K	SNTC-24X7X4 Cisco Business Edition 6000M Svr (M4), E
1	CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America
1	CIT-PSU1-770W	770W AC Hot-Plug Power Supply for 1U C-Series Rack Server
1	CIT-CPU-E52630D	2.40 GHz E5-2630 v3/85W 8C/20MB Cache/DDR4 1866MHz
1	R2XX-RAID5	Enable RAID 5 Setting
1	CIT-MRAID12G	Cisco 12G SAS Modular Raid Controller
1	CIT-MRAID12G-1GB	Cisco 12Gbps SAS 1GB FBWC Cache module (Raid 0/1/5/6)
1	VMW-VS6-HYPPLS-K9	Embedded License, Cisco UC Virt. Hypervisor Plus 6.x (2-cpu)
6	CIT-HD300G10K12G	300GB 12G SAS 10K RPM SFF HDD
2	CIT-MR-1X161RV-A	16GB DDR4-2400-MHz RDIMM/PC4-19200/single rank/x4/1.2v
1	UCSC-PSU1-770W=	770W AC Hot-Plug Power Supply for 1U C-Series Rack Server
1	CAB-9K12A-NA=	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America
1	ISR4321-V/K9	Cisco ISR 4321 Bundle, w/UC License, CUBE-10
1	CON-SNTP-ISR4321V	SNTC-24X7X4 Cisco ISR 4321 UC Bundle, PVDM4-32, UC L
1	SL-4320-IPB-K9	IP Base License for Cisco ISR 4320 Series
1	SL-4320-UC-K9	Unified Communication License for Cisco ISR 4320 Series
1	PWR-4320-AC	AC Power Supply for Cisco ISR 4320
1	CAB-AC-C5	AC Power Cord, Type C5, US, Canada
1	MEM-FLSH-4G	4G Flash Memory for Cisco ISR 4300 (Soldered on motherboard)
1	MEM-4320-4G	4G DRAM for Cisco ISR 4320 (Soldered on motherboard)
2	FL-CUBEE-5	Unified Border Element Enterprise License - 5 sessions
1	SISR4300UK9-316S	Cisco ISR 4300 Series IOS XE Universal

1	FL-SRST	Cisco Survivable Remote Site Telephony (SRST) License
2	FL-CME-SRST-25	SRST-25 Seat License (CME uses CUCME Phone License ONLY)
1	NIM-2FXS	2-Port Network Interface Module - FXS, FXS-E and DID
1	NIM-1MFT-T1/E1	1 port Multiflex Trunk Voice/Clear-channel Data T1/E1 Module
1	PVDM4-32	32-channel DSP module
50	CP-7841-K9=	Cisco UC Phone 7841
1	R-CBE6K-K9	Cisco Business Edition 6000-Electronic SW Delivery-Top Level
1	CON-ECMU-RCBE6KK	SWSS UPGRADES Cisco Business Editi
50	JABBER-DESKTOP	Jabber for Desktop for PC and Mac
1	JABBER-DSK-K9-RTU	Jabber for Desktop Right to Use
1	BE6K-PAK	Cisco Business Edition 6000 - PAK - Single Fulfillment
1	LIC-EXP-E-PAK	Expressway Series, Expressway-E PAK
4	LIC-EXP-GW	Enable GW Feature (H323-SIP)
2	LIC-EXP-E	Enable Expressway-E Feature Set
2	LIC-EXP-TURN	Enable TURN Relay Option
2	LIC-EXP-AN	Enable Advanced Networking Option
4	LIC-SW-EXP-K9	License Key Software Encrypted
4	LIC-EXP-SERIES	Enable Expressway Series Feature Set
2	EXPWY-VE-E-K9	Cisco Expressway-E Server, Virtual Edition
2	EXPWY-VE-C-K9	Cisco Expressway-C Server, Virtual Edition
50	LIC-EXP-DSK	Expressway Desktop Endpoint License
1	SW-EXP-8.X-K9	Software Image for Expressway with Encryption, Version X8
1	BE6K-SW-11.5	Business Edition 6000 v11.5 export restricted software
15	BE6K-UCL-ENH	Cisco Business Edition 6000 - Enhanced User Connect License
15	UCM-11X-ENH-UCL	BE6K UCM 11X Enhanced User Connect Lic - Single Fulfillment
15	CON-ECMU-UCMENHUC	SWSS UPGRADES BE6K UCM 10X Enhance
2	UCXN-11X-SCPORTS	BE6K - Unity Connection 11x - VM Speech Connect Ports
1	BE6K-UXL-START	BE6K Starter Pack - Single Fulfillment Enforcement
1	BE6K-START-UCL35	BE6000 Starter Bundle with 35 UCL Enh and 35 vmail Licenses
15	BE6K-UCL-VM	Cisco Business Edition 6000- Voicemail/Unified Messaging Lic
15	UCN-11X-VM-UCL	BE6000 Unity Connection 11x Basic Voicemail License
15	CON-ECMU-UCN10XVM	SWSS UPGRADES BE6K - Unity Connect
1	BE-11X-UCL-STR	BE6000 v11 UCL Starter licenses

1	CON-ECMU-BE1U1XCU	SWSS UPGRADES BE6000 v11 UCL Starter licenses
1	WS-C2960X-48LPS-L	Catalyst 2960-X 48 GigE PoE 370W, 4 x 1G SFP, LAN Base
1	CON-SNT-WSC248SL	SNTC-8X5XNBD Catalyst 2960-X 48 G
1	CAB-16AWG-AC	AC Power cord, 16AWG
1	C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module
1	CAB-STK-E-0.5M	Cisco FlexStack 50cm stacking cable
1	WS-C2960X-24PS-L	Catalyst 2960-X 24 GigE PoE 370W, 4 x 1G SFP, LAN Base
1	CON-SNT-WSC224SL	SNTC-8X5XNBD Catalyst 2960-X 24 G
1	CAB-16AWG-AC	AC Power cord, 16AWG
1	C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module
1	CAB-STK-E-0.5M	Cisco FlexStack 50cm stacking cable

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

None

Category: Private Cloud

601458

Company's Responsibilities and Included Features

Description:
The ReliaCloud dedicated blade service delivers a Client dedicated Intel based server blade solution with network connectivity into the ReliaCloud fiber channel storage and Ethernet networks with a fixed configuration of system resources. The dedicated blade model is designed to support a single x86, -x64 based operating system environment or a hypervisor such as VMware , Hyper-V or Oracle VM.

Specifications and Services:

- Server Configuration
  - Cisco B200 M4 blade server with dual Intel Xeon E5-2667 v4 processors (8 Cores x.3.2GHz)
  - 256 GB RAM.
  - All storage will be Storage Area Network (SAN) based including operating system that will boot from SAN
  - Dual four (4) Port 10 Gigabit Ethernet, Fiber Channel over Ethernet (FCoE) virtual interface cards

Blade Chassis and ReliaCloud Network Connectivity

- The dedicated blade server is housed in a shared blade chassis which provides:
  - Redundant power to the blade server.
  - Redundant cooling to the blade server.
  - Fiber channel connectivity to the ReliaCloud storage solutions.
  - Ethernet connectivity to the core ReliaCloud LAN, provisioned as Client dedicated VLAN s for outbound connectivity to the Client or internal connectivity between servers or to other ReliaCloud services.

Dedicated Blade Management

Company will provide management of the dedicated blade, which includes:

- Hardware Management
  - Triage, diagnosis and repair of blade, chassis and attached network hardware issues.
  - Manage hardware replacement and or repair with hardware vendor.
  - Maintain maintenance agreements for blade, chassis and attached network hardware.
  - Maintain blade profile.
  - Company will provide replacement blades within 24 hours of failure.
  - No server bare metal or console/KVM access will be granted to Client. Company will provide management of all tasks that require bare metal or UCS console access to the server.

Support and Access

- Access to 24x7 expert-to-expert engineering support.
- Provide monitoring visibility into the performance of the dedicated blade.
- Provide notification to Client of any critical blade or network level issues.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of any service requirements, changes or modifications.
- Operating system and application licensing and supporting maintenance.
- Ownership and management of Client applications.
- Ownership and management of blade operating system,
- Subscription to Company enterprise firewall services is required,
- No disk storage is included in the server.
- VPN or WAN connectivity to server through the ReliaCloud network.

601686 ReliaCloud Hosted EDGE DR Node - HMN32C768

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services.

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged cluster

Company's Responsibilities and Included Features

ReliaCloud Hosted EDGE DR Node - HMN32C768 (DR Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS for the purpose of providing disaster recovery (DR) solutions. DR Nodes must minimally belong to a Cluster configured with at least three (3) Nodes. DR Nodes are dedicated to the Client for their exclusive use. DR Nodes may be leveraged as a replication target and failed over to, based upon a Client defined event.

DR Node service is not inclusive of replication technology management.

DR Node physical specifications

Company will provide a DR Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon processors 6226R (2.9 GHz, 16 cores), 32 cores total
- 768 GB RAM
- Hybrid performance disk configuration consisting of 24TB HDD and 7.68TB SSD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity such as but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

DR Node software specifications

Company will provide a DR Node that meets or exceeds the following software specifications:

- Nutanix AOS Ultimate
- Nutanix Prism Pro

DR Node hosting specifications

- Provide a secure four-sided locking cabinet to host the DR Node. Cabinets are multi-tenant and under the exclusive control of Company
- Provide continuous power to the DR Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all physical moves, adds and changes
- Provide a two (2) network connections (LAN) that support up to 25 Gbps port speeds

AOS Administration

Company supports administration of the following base features of AOS. Base features are Company s definition of the core services necessary to operate and manage Nutanix AOS. Nutanix AOS will contain features that are outside of Company s base definition and may be available under a different ItemID. Management is quantified as per Node that participates within the Cluster.

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster grown/shrink
    - Nutanix Volumes
    - Compression
    - Deduplication
    - Erasure coding (EC-X)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
    - Availability domain Block/rack awareness
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements

Pulse
- Cluster health

Cluster and Node Incident Triage and Troubleshooting

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting of Node hardware or operating system incidents
- Document user issues and AOS errors

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Upgrades to a new major version of the AOS are out of scope for this SOW, but may be provided by Company under a separate time-and-material statement of work

Block and Node Maintenance Management

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Periodic reviews of critical patches

Block and Node Maintenance Management includes:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of any service requirements, changes or modifications.
- Provide approved maintenance window for patching
- Application licensing and supporting maintenance including the hypervisor (if not AHV), virtual machine operating system licensing and support maintenance.
- Ownership and management of guest VM applications and operating systems support
- Backup services
- Management of network devices
- Migrating VMs onto or off the platform
- Disaster recovery solution and associated services
- Management of third-party enhancement tools, utilities or applications

Minimum Requirements

DR Node must belong within a Cluster containing at least three (3) Nodes.

Business Continuity / Disaster Recovery Plan

Client Business Continuity / Disaster Recovery plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation is out of scope for this engagement.

DR Configuration

- DR recovery retention window
- Server startup sequencing and startup delay
- Network mapping
- Server re-IP plan (if applicable)

Virtualization Platform

- Virtualization platform sizing with sufficient capacity in the source (production) and target (DR) data centers
- Capacity must include the necessary capacity for the DR replication software servers/virtual appliances
- Virtualization software (if not AHV) on which the virtual machine being managed is run
- Management of virtualization platform

Replication Network

- A network connection between the primary and recovery sites with sufficient bandwidth to accommodate the recovery point objective (RPO) requirements.

Applications and Client-Side DR Configuration and Testing

- Maintain DR test and failover procedures for all databases and applications existing on the servers included in the DR plan
- Database and application management and reconfiguration during DR testing or failover
- Configurations of end-user devices and/or Client infrastructure required to allow end users to access the environment.
- Conduct functional and data validation testing during server failover testing.

601687 ReliaCloud Hosted EDGE DR Node - HMN32C768i

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services.

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged cluster

Company's Responsibilities and Included Features

ReliaCloud Hosted EDGE DR Node - HMN32C768 (DR Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS for the purpose of providing disaster recovery (DR) solutions. DR Nodes must minimally belong to a Cluster configured with at least three (3) Nodes. DR Nodes are dedicated to the Client for their exclusive use. DR Nodes may be leveraged as a replication target and failed over to, based upon a Client defined event.

DR Node service is not inclusive of replication technology management.

DR Node physical specifications

Company will provide a DR Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon processors 6226R (2.9 GHz, 16 cores), 32 cores total
- 768 GB RAM
- Hybrid performance disk configuration consisting of 24TB HDD and 7.68TB SSD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity such as but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

DR Node software specifications

Company will provide a DR Node that meets or exceeds the following software specifications:

- Nutanix AOS Ultimate
- Nutanix Prism Pro

DR Node hosting specifications

- Provide a secure four-sided locking cabinet to host the DR Node. Cabinets are multi-tenant and under the exclusive control of Company
- Provide continuous power to the DR Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all physical moves, adds and changes
- Provide a two (2) network connections (LAN) that support up to 25 Gbps port speeds

AOS Administration

Company supports administration of the following base features of AOS. Base features are Company s definition of the core services necessary to operate and manage Nutanix AOS. Nutanix AOS will contain features that are outside of Company s base definition and may be available under a different ItemID. Management is quantified as per Node that participates within the Cluster.

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster grown/shrink
    - Nutanix Volumes
    - Compression
    - Deduplication
    - Erasure coding (EC-X)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
    - Availability domain Block/rack awareness
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)

- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

Cluster and Node Incident Triage and Troubleshooting

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting of Node hardware or operating system incidents
- Document user issues and AOS errors

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Upgrades to a new major version of the AOS are out of scope for this SOW, but may be provided by Company under a separate time-and-material statement of work

Block and Node Maintenance Management

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Periodic reviews of critical patches

Block and Node Maintenance Management includes:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of any service requirements, changes or modifications.
- Provide approved maintenance window for patching
- Application licensing and supporting maintenance including the hypervisor (if not AHV), virtual machine operating system licensing and support maintenance.
- Ownership and management of guest VM applications and operating systems support
- Backup services
- Management of network devices
- Migrating VMs onto or off the platform
- Disaster recovery solution and associated services
- Management of third-party enhancement tools, utilities or applications

Minimum Requirements

DR Node must belong within a Cluster containing at least three (3) Nodes.

Business Continuity / Disaster Recovery Plan

Client Business Continuity / Disaster Recovery plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation is out of scope for this engagement.

DR Configuration

- DR recovery retention window
- Server startup sequencing and startup delay
- Network mapping
- Server re-IP plan (if applicable)

Virtualization Platform

- Virtualization platform sizing with sufficient capacity in the source (production) and target (DR) data centers
- Capacity must include the necessary capacity for the DR replication software servers/virtual appliances
- Virtualization software (if not AHV) on which the virtual machine being managed is run
- Management of virtualization platform

Replication Network

- A network connection between the primary and recovery sites with sufficient bandwidth to accommodate the recovery point objective (RPO) requirements.

Applications and Client-Side DR Configuration and Testing

- Maintain DR test and failover procedures for all databases and applications existing on the servers included in the DR plan
- Database and application management and reconfiguration during DR testing or failover
- Configurations of end-user devices and/or Client infrastructure required to allow end users to access the environment.
- Conduct functional and data validation testing during server failover testing.

601738 ReliaCloud EDGE Node 1075s - HMAHV

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Node 1075s - HMAHV (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE Nodes minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- One (1) Intel Gold processor 6226R (2.9 GHz, 16 cores), 16 cores total
- 384 GB RAM
- Hybrid performance disk configuration consisting of 24TB HDD and 7.68TB SSD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix AOS Ultimate
- Nutanix Prism Pro

Node hosting specifications

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 10 Gbps port speeds

AOS Administration

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster

level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable timeframe based on the severity of the updates, patches or upgrades, Client waives any and all claims against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updates and upgrades are up to date. If patching, updating or upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time updating, patching or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades, updates or patches.

Block and Node Maintenance Management

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded

from this scope.
- VM automated resource scheduling
- VM affinity rules
- Virtual network configuration
- Host profiles
- VM high availability
- Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable timeframe based on the severity of the update, upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updating and upgrades are up to date. If patching, updating or upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time patching, updating or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for updates, upgrades and/or patches.

Co-administration

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
  - Cluster and VM performance and analysis
  - Cluster and health and availability
  - Cluster capacity and trend info
  - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
  - Create, delete and modify VMs
  - Execute snapshots and restorations
  - Add VMs to catalog
  - Import, add, create and delete images to catalog
  - Create and modify data protection and recovery policies

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

601741 ReliaCloud EDGE Node 1075s - HMESX

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

VMware ESXi: VMware's hypervisor platform

Company's Responsibilities and Included Features

ReliaCloud EDGE Node 1075s HMESX (EDGE Node) service is comprised of hardware, software and a base level of

management services for the Nutanix AOS and VMware ESXi. Nodes must minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- One (1) Intel Gold processor 6226R (2.9 GHz, 16 cores), 16 cores total
- 384 GB RAM
- Hybrid performance disk configuration consisting of 24TB HDD and 7.68TB SSD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix AOS Ultimate
- Nutanix Prism Pro
- VMware ESXI is not included within this scope, but it is available from Company under a separate ItemID.

Node hosting specifications

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 10 Gbps port speeds

AOS Administration

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience

        - Data path redundancy
        - Tunable redundancy factor
    - Security
        - Client authentication
        - Cluster lockdown
        - Data-at-rest encryption (software-based and self-encrypting drives)
    - Management and Analytics
        - Prism Central and Prism Elements
        - Pulse
        - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable timeframe based on the severity of the updates, patches or upgrades, Client waives any and all claims against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updates and upgrades are up to date. If patching, updating or upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time updating, patching or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades, updates or patches.

Block and Node Maintenance Management

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

VMware System Administration

Company will support administration of the following base features of VMware ESXi:

- Perform preventative maintenance
- Perform emergency maintenance
- Provide performance tuning
- Perform server health checks
- Perform file system maintenance
- Provision Virtual Machines (VM)
- Manage basic vSwitch network
- Manage advanced network switching (i.e. VMware vDS or other vendor supported 3rd party switch)
- Manage basic vStorage network
- Manage VMware server through vCenter
- Manage vCenter application
- Administer built-in VMware dependency components
- Provide utilization reporting

LAN management of the virtual switch is specifically excluded from this scope of Services.

VMware ESXi Triage and Troubleshooting

- Triage of VMware ESXi incidents
- Troubleshoot and work to resolve VMware ESXi system incidents
- Document VMware ESXi system issues and errors

VMware ESXi Patching, Updates and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the VMware ESXi software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable timeframe based on the severity of the update, upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updates and upgrades are up to date. If patching, updating or upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time patching, updating or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for updates, upgrades or patches.

Co-administration

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into vCenter and general visibility into the Cluster metrics and configuration settings such as as:
    - Cluster and VM performance and analysis
    - Cluster and health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog

Create and modify data protection and recovery policies

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications

- Manage third-party ESX enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AOS is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees, acknowledges, and understands that the actual manufacture of the VMware ESXi is by VMware, Inc. and its provision and performance may be subject to change as determined by VMware, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.
- Client agrees that VMware ESXi offerings provided herein are subject to the VMware Services End User License Agreement available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf and privacy policy located at https://www.vmware.com/help/privacy.html, which are hereby incorporated into this Statement of Work.

601746 ReliaCloud EDGE Dedicated Reserved Node 8H - 8035r1

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Dedicated Reserved Node 8035r1 (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 6226R (2.9 GHz, 16 cores), 32 cores total
- 768 GB RAM
- Hybrid performance disk configuration consisting of 48TB HDD and 15.36TB SSD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE Activated Reserved Node Rate (separate Itemd ID), until Client submits a service request for a Reserved Node to be:

  A) Removed from the Cluster, at which point the Reserved Node will remain available and billed (commencing the following month) at its Reserved Node rates;

  or

  B) Elevated to production status, at which point the Reserved Node will become part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node 8035 rate (commencing the following month).

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE Node 8035r1 Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s Activated Reserved Node 8035r1 Services
- Notify Company to request Node activations, deactivation or changes in use to production status

601869 ReliaCloud EDGE Node 8035r1 - HMAHV

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Node 8035r1 - HMAHV (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE Nodes minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 6226R (2.9 GHz, 16 cores), 32 cores total
- 768 GB RAM
- Hybrid performance disk configuration consisting of 48TB HDD and 15.36TB SSDD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix AOS Ultimate
- Nutanix Prism Pro

Node hosting specifications

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters

        - Data tiering
        - Inline compression
        - Inline performance deduplication
        - Online Cluster growth
        - Compression
        - Deduplication
        - Erasure coding (EC-X) *
    - Nutanix Volumes Management
        - Creation of iSCSI volume group(s)
        - Management of volume groups
        - Management of client iSCSI initiators
        - Management of iSCSI data services
        - Configure Bare Metal Nodes for IP addressing
            - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
    - Infrastructure Resilience
        - Data path redundancy
        - Tunable redundancy factor
    - Security
        - Client authentication
        - Cluster lockdown
        - Data-at-rest encryption (software-based and self-encrypting drives)
    - Management and Analytics
        - Prism Central and Prism Elements
        - Pulse
        - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable timeframe based on the severity of the updates, patches or upgrades, Client waives any and all claims against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updates and upgrades are up to date. If patching, updating or upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time updating, patching or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades, updates or patches.

Block and Node Maintenance Management

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable timeframe based on the severity of the update, upgrade or patch, Client waives any and all claims

against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updating and upgrades are up to date. If patching, updating or upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time patching, updating or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for updates, upgrades and/or patches.

Co-administration

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
  - Cluster and VM performance and analysis
  - Cluster and health and availability
  - Cluster capacity and trend info
  - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
  - Create, delete and modify VMs
  - Execute snapshots and restorations
  - Add VMs to catalog
  - Import, add, create and delete images to catalog
  - Create and modify data protection and recovery policies

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan

- Client is responsible for all disaster recovery solutions and associated services

- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

601878 ReliaCloud EDGE Node 8035r1 - HMESX

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

VMware ESXi: VMware's hypervisor platform

Company's Responsibilities and Included Features

ReliaCloud EDGE Node 8035r1 HMESX (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and VMware ESXi. Nodes must minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 6226R (2.9 GHz, 16 cores), 32 cores total
- 768 GB RAM
- Hybrid performance disk configuration consisting of 48TB HDD and 15.36TB SSD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix AOS Ultimate
- Nutanix Prism Pro
- VMware ESXI is not included within this scope, but it is available from Company under a separate ItemID.

Node hosting specifications

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.

- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable timeframe based on the severity of the updates, patches or upgrades, Client waives any and all claims against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updates and upgrades are up to date. If patching, updating or

upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time updating, patching or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades, updates or patches.

Block and Node Maintenance Management

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

VMware System Administration

Company will support administration of the following base features of VMware ESXi:

- Perform preventative maintenance
- Perform emergency maintenance
- Provide performance tuning
- Perform server health checks
- Perform file system maintenance
- Provision Virtual Machines (VM)
- Manage basic vSwitch network
- Manage advanced network switching (i.e. VMware vDS or other vendor supported 3rd party switch)
- Manage basic vStorage network
- Manage VMware server through vCenter
- Manage vCenter application
- Administer built-in VMware dependency components
- Provide utilization reporting

LAN management of the virtual switch is specifically excluded from this scope of Services.

VMware ESXi Triage and Troubleshooting

- Triage of VMware ESXi incidents
- Troubleshoot and work to resolve VMware ESXi system incidents
- Document VMware ESXi system issues and errors

VMware ESXi Patching, Updates and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the VMware ESXi software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable time frame based on the severity of the update, upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updates and upgrades are up to date. If patching, updating or

upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time patching, updating or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for updates, upgrades or patches.

Co-administration

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into vCenter and general visibility into the Cluster metrics and configuration settings such as as:
  - Cluster and VM performance and analysis
  - Cluster and health and availability
  - Cluster capacity and trend info
  - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
  - Create, delete and modify VMs
  - Execute snapshots and restorations
  - Add VMs to catalog
  - Import, add, create and delete images to catalog
  - Create and modify data protection and recovery policies

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications

- Manage third-party ESX enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AOS is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees, acknowledges, and understands that the actual manufacture of the VMware ESXi is by VMware, Inc. and its provision and performance may be subject to change as determined by VMware, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.
- Client agrees that VMware ESXi offerings provided herein are subject to the VMware Services End User License Agreement available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf and privacy policy located at https://www.vmware.com/help/privacy.html, which are hereby incorporated into this Statement of Work.

601961 ReliaCloud EDGE Node 8070 - HMESX

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

VMware ESXi: VMware's hypervisor platform

Company's Responsibilities and Included Features

ReliaCloud EDGE Node 8070 HMESX (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and VMware ESXi. Nodes must minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 6226R (2.9 GHz, 16 cores), 32 cores total
- 768 GB RAM
- All flask disk configuration consisting of 30.72 TB of NVMe drives

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix AOS Ultimate

- Nutanix Prism Pro
- VMware ESXI is not included within this scope, but it is available from Company under a separate ItemID.

Node hosting specifications

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the AOS software (including major upgrades) will be conducted at Company s discretion and in

accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable timeframe based on the severity of the updates, patches or upgrades, Client waives any and all claims against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updates and upgrades are up to date. If patching, updating or upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time updating, patching or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades, updates or patches.

Block and Node Maintenance Management

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

VMware System Administration

Company will support administration of the following base features of VMware ESXi:

- Perform preventative maintenance
- Perform emergency maintenance
- Provide performance tuning
- Perform server health checks
- Perform file system maintenance
- Provision Virtual Machines (VM)
- Manage basic vSwitch network
- Manage advanced network switching (i.e. VMware vDS or other vendor supported 3rd party switch)
- Manage basic vStorage network
- Manage VMware server through vCenter
- Manage vCenter application
- Administer built-in VMware dependency components
- Provide utilization reporting

LAN management of the virtual switch is specifically excluded from this scope of Services.

VMware ESXi Triage and Troubleshooting

- Triage of VMware ESXi incidents
- Troubleshoot and work to resolve VMware ESXi system incidents
- Document VMware ESXi system issues and errors

VMware ESXi Patching, Updates and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the VMware ESXi software (including major upgrades) will be conducted at Company s discretion

and in accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable time frame based on the severity of the update, upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updates and upgrades are up to date. If patching, updating or upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time patching, updating or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for updates, upgrades or patches.

Co-administration

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into vCenter and general visibility into the Cluster metrics and configuration settings such as as:
  - Cluster and VM performance and analysis
  - Cluster and health and availability
  - Cluster capacity and trend info
  - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
  - Create, delete and modify VMs
  - Execute snapshots and restorations
  - Add VMs to catalog
  - Import, add, create and delete images to catalog
  - Create and modify data protection and recovery policies

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications

- Manage third-party ESX enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AOS is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees, acknowledges, and understands that the actual manufacture of the VMware ESXi is by VMware, Inc. and its provision and performance may be subject to change as determined by VMware, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.
- Client agrees that VMware ESXi offerings provided herein are subject to the VMware Services End User License Agreement available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf and privacy policy located at https://www.vmware.com/help/privacy.html, which are hereby incorporated into this Statement of Work.

601972 ReliaCloud EDGE Bare Metal Node HPE DL380 Gen10 8SFF

Company's Responsibilities and Included Features

Provide a HPE DL380 Gen10 8SFF CTO Server "Bare Metal Node" on a monthly subscription basis.

Bill of Materials

Ln#	Qty	Part #	Description
1	1	868703-B21	HPE DL380 Gen10 8SFF CTO Server
2	1	P24476-L21	Intel Xeon-G 6256 FIO Kit for DL380 G10
3	6	P00930-B21	HPE 64GB 2Rx4 PC4-2933Y-R Smart Kit
4	1	P12965-B21	HPE NS204i-p Gen10+ Boot Ctrlr
5	1	817709-B21	HPE 10/25GbE 2p FLR-SFP28 BCM57414 Adptr
6	2	845398-B21	HPE 25Gb SFP28 SR 100m Transceiver
7	1	867810-B21	HPE DL38X Gen10 High Perf Fan
8	2	865414-B21	HPE 800W FS Plat Ht Plg LH Pwr Sply Kit
9	1	BD505A	HPE iLO Adv 1-svr Lic 3yr Support
10	1	720863-B21	HPE 2U SFF BB Rail Kit
11	1	H7J34A3	HPE 3Y Foundation Care 24x7 Service

Server Hardware Management

Server hardware management includes:

- Triage, diagnosis and work to resolve hardware issues
- Management of hardware replacement and/or repair with applicable hardware vendor

- Analysis of any hardware additions or upgrades
- Application of hardware firmware updates as necessary

Repair and SLO

- The Service Level Objective (SLO) for repair or replacement is next business day or better.

Service Requirements

- Bare Metal Node must be attached to a Company approved ReliaCloud Cluster
- Client must contract for ReliaCloud Extend services for Bare Metal Node physical hosting and network services
- Bare Metal Node must attach via (four) 4 x 25Gbps network connections
- Client must contract for hypervisor or dedicated operating system management on the Bare Metal Node
- Bare Metal Node operating system must be supported by Nutanix for compatibility with Nutanix Volumes

Nutanix Volumes Management

- Creation of iSCSI volume group(s)
- Management of volume groups
- Management of client iSCSI initiators
- Management of iSCSI data services
- Configure Bare Metal Nodes for IP addressing
- If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Equipment must be colocated (housed) within one of the Company s data centers.

602673 ReliaCloud EDGE Bare Metal Node HPE DL360 Gen10 4SFF

Company's Responsibilities and Included Features

Provide a HPE DL360 Gen10 4SFF CTO Server "Bare Metal Node" on a monthly subscription basis.

Bill of Materials

Ln#	Qty	Part #	Description
1	1	P18229-B21	HPE DX360 Gen10 4LFF CTO Svr
2	1	P24662-L21	HPE DX360 Gen10 6256 FIO Kit
3	6	P18453-B21	HPE DX 64G 2Rx4 PC4-2933Y-R Smt FIO Kit
4	2	P18737-B21	HPE DX 1.92TB SATA RI LFF SCC DS FIO SSD
5	1	P18462-B21	HPE DX Eth 10/25Gb 2p 640SFP28 FIO Adptr
6	1	P18461-B21	HPE DX Eth 10/25Gb 2p 640FLR FIO Adptr
7	4	P18413-B21	HPE DX 25Gb SFP28 SR 100m FIO XCVR
8	2	P18226-B21	HPE DX 500W FS Plat Ht Plg LH FIO PS Kit
9	2	R1C65A	HPE C13-C14 IN 250V 2m Blk Jumper Cord
10	1	R6T15A	Nutanix AOS LTS FIO SW for HPE
11	1	P23849-B21	HPE DX 1U Gen10 LFF EI FIO Rail Kit

12	1	HN4Z0E	HPE 3Y 24x7 DX360 Gen10 HW SVC

Server Hardware Management

Server hardware management includes:

- Triage, diagnosis and work to resolve hardware issues
- Management of hardware replacement and/or repair with applicable hardware vendor
- Analysis of any hardware additions or upgrades
- Application of hardware firmware updates as necessary

Repair and SLO

- The Service Level Objective (SLO) for repair or replacement is next business day or better.

Service Requirements

- Bare Metal Node must be attached to a Company approved ReliaCloud Cluster
- Client must contract for ReliaCloud Extend services for Bare Metal Node physical hosting and network services
- Bare Metal Node must attach via (four) 4 x 25Gbps network connections
- Client must contract for hypervisor or dedicated operating system management on the Bare Metal Node
- Bare Metal Node operating system must be supported by Nutanix for compatibility with Nutanix Volumes
- If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Equipment must be colocated (housed) within one of the Company s data centers.

602746 ReliaCloud EDGE Node GPC.1607H.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Node GPC 1607H.A (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE Nodes minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- One (1) Intel Xeon Gold processor 6326 (2.9 GHz, 16 cores), 16 cores total
- 512 GB RAM
- Hybrid performance disk configuration consisting of 24 TB HDD and 7.68 TB SDD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix AOS Ultimate
- Nutanix Prism Pro

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
    - Cluster and VM performance and analysis
    - Cluster and health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection and recovery policies

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems support

- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

602747 ReliaCloud EDGE Node GPC.2407H.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Node GPC 2407H.A (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE Nodes minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 5317 (3 GHz, 12 cores), 24 cores total
- 512 GB RAM
- Hybrid performance disk configuration consisting of 24 TB HDD and 7.68 TB SDD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix AOS Ultimate
- Nutanix Prism Pro

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents

Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
  - Cluster and VM performance and analysis
  - Cluster and health and availability
  - Cluster capacity and trend info
  - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
  - Create, delete and modify VMs
  - Execute snapshots and restorations
  - Add VMs to catalog
  - Import, add, create and delete images to catalog
  - Create and modify data protection and recovery policies

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

602748 ReliaCloud EDGE Node GPC.3215H.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Node GPC 3215H.A (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE Nodes minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 6346 (3.1 GHz, 16 cores), 32 cores total
- 1024 GB RAM
- Hybrid performance disk configuration consisting of 48 TB HDD and 15.36 TB SDD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix AOS Ultimate

- Nutanix Prism Pro

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)

- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
  - Cluster and VM performance and analysis
  - Cluster and health and availability
  - Cluster capacity and trend info
  - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
  - Create, delete and modify VMs
  - Execute snapshots and restorations
  - Add VMs to catalog
  - Import, add, create and delete images to catalog
  - Create and modify data protection and recovery policies

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

Client is responsible for all disaster recovery solutions and associated services

- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

602749 ReliaCloud EDGE Node GPC.3230H.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Node GPC 3230H.A (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE Nodes minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 6346 (3.1 GHz, 16 cores), 32 cores total
- 1024 GB RAM
- Hybrid performance disk configuration consisting of 64 TB HDD and 30.72 TB SDD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix AOS Ultimate
- Nutanix Prism Pro

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.

- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows

- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
  - Virtual Machine (VM) centric snapshots and clones
  - VM-centric Storage QoS
  - VM Flash Mode
- Data Protection
  - Application consistent snapshots
  - Local snapshots
  - Self-service restores
  - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
  - VM management. VM s operating system management and application management is specifically excluded from this scope.
  - VM automated resource scheduling
  - VM affinity rules
  - Virtual network configuration
  - Host profiles
  - VM high availability
  - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
  - Cluster and VM performance and analysis
  - Cluster and health and availability
  - Cluster capacity and trend info
  - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
  - Create, delete and modify VMs
  - Execute snapshots and restorations
  - Add VMs to catalog
  - Import, add, create and delete images to catalog
  - Create and modify data protection and recovery policies

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

602750 ReliaCloud EDGE Node FIL.2415H.A

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

File Server Virtual Machine (FSVM): A virtual machine that runs as part of the Nutanix Files file server service.

ICAP: Internet Content Adaptation Protocol (ICAP) is a lightweight protocol designed to offload processing of Internet-based content to dedicated servers. The goal of ICAP, a lightweight HTTP-based RPC protocol, is to offload tasks like antivirus scanning onto specialized servers to increase network throughput.

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Nutanix Files (Files): A software-defined scale-out file storage solution designed to address a wide range of use cases, including but not limited to: support for Linux and Windows home directories, user profiles and department shares.

SMB: Server Message Block, is a network protocol used by Windows-based computers that allows systems within the same network to share files

Company's Responsibilities and Included Features

ReliaCloud EDGE FIL.2415H.A Node (EDGE Files Node) service is comprised of hardware and a base level of management services for the Nutanix AOS and Nutanix Files Software. EDGE Files Nodes minimally belong to a Cluster configured with at least four (4) EDGE Files Nodes. EDGE Files Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Files Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 5317R (3 GHz, 12 cores), 24 cores total
- 512 GB RAM
- Disk configuration consisting of 15.36 TB SSD
- Disk configuration consisting of 120 TB HDD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption as well as the types of workloads that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Files Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility

- Maintain physical security of the cabinet
- Provide all EDGE Files Node physical moves, adds and changes
- Provide four (4) network LAN connections that support up to 25 Gbps port speeds.

AOS Administration:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
- Management and Analytics
    - Prism Elements

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals. Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor

Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

Nutanix Files Administration:

Company will support administration of the following functions:

- File Server Management
  - Creating a file server
  - Maintain the Files Cluster
  - File server cloning
  - Encryption settings
  - Antivirus (AV) scanning (SMB Only)
  - Provide recommendations on File Server Virtual Machines (FSVMs) infrastructure sizing including storage requirements based upon workload.
- Files Optimization
  - Performance optimization
  - File system compression
- Share and Export Management
  - Creating file shares
  - Creating exports
  - Multiprotocol support
- Domain Configuration Management
  - Domain joining
  - Updating Domain Name System (DNS) entries
  - Disjoint domain management
- Directory and User Management
  - Updating Files directory services
  - Management of user mappings
  - Managing user roles
  - Management of user quotas
- Data Recovery Management
  - Management of protection domain and snapshot schedule
  - Support for Files asynchronous replication with a minimum 1-hour recovery point objective
  - Upon Client request, activation of disaster recovery of File Server Virtual Machines (FSVMs)
  - Configuration for high availability of FSVMs
  - Configuration of self-service restore (SSR) and snapshot schedule parameters

Nutanix Files analytics is not within scope of this ItemID. Files analytics support is available under a separate ItemID.

Files Triage and Troubleshooting:

- Triage of Files system incidents
- Troubleshoot and work to resolve Files system incidents
- Document Files system issues and error

Nutanix Files analytics is not within scope of this ItemID. Files analytics support is available under a separate ItemID.

Files Patching, Updates and Upgrades:

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of Updates during Company defined maintenance windows
- Periodic upgrades to the Files software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices during Client approved maintenance windows triage of Files system incidents

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
  - Files dashboard
  - File Server alerts and notifications
  - File Server events
- Self-service management
  - Self-service File restoration
  - Execute snapshots and restorations

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Subscribe to Company Nutanix Files Software service EDGE Files Node under ItemID 60187.
- Manage end user Files share access management and usage
- For anti-virus scanning support, provide ICAP compatible anti-virus software
- Migration of Files data onto and off of the Cluster
- Open necessary network and firewall ports to provide Company access to Management VMs
- Provide VPN termination point for Company to access Client s environment
- Perform all data backup
- Provide Company with a snapshot policy
- Execute file level self-service restorations
- Provide a directory service and credentials to integrate into the file service

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

602752 ReliaCloud EDGE Node HPC.3661N.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Node HPC 3661N.A (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE Nodes minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 6353 (3 GHz, 18 cores), 36 cores total
- 1024 GB RAM
- Disk configuration consisting of 61.44 TB NVME

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix AOS Ultimate
- Nutanix Prism Pro

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide four (4) network LAN connections that support up to 25 Gbps port speeds

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression

        - Deduplication
        - Erasure coding (EC-X) *
    - Nutanix Volumes Management
        - Creation of iSCSI volume group(s)
        - Management of volume groups
        - Management of client iSCSI initiators
        - Management of iSCSI data services
        - Configure Bare Metal Nodes for IP addressing
            - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
    - Infrastructure Resilience
        - Data path redundancy
        - Tunable redundancy factor
    - Security
        - Client authentication
        - Cluster lockdown
        - Data-at-rest encryption (software-based and self-encrypting drives)
    - Management and Analytics
        - Prism Central and Prism Elements
        - Pulse
        - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
    - Cluster and VM performance and analysis
    - Cluster and health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection and recovery policies

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.

- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

602759 ReliaCloud EDGE Node GPC.1607H.E

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

VMware ESXi: VMware's hypervisor platform

Company's Responsibilities and Included Features

ReliaCloud EDGE GPC.1607H.E (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and VMware ESXi. Nodes must minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- One (1) Intel Xeon Gold processors 6326 (2.9 GHz, 16 cores), 16 cores total
- 512 GB RAM
- Hybrid performance disk configuration consisting of 24TB HDD and 7.68TB SSD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix AOS Ultimate
- Nutanix Prism Pro
- VMware ESXi is not included within this scope, but it is available from Company under a separate ItemID.

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups

        - Management of client iSCSI initiators
        - Management of iSCSI data services
        - Configure Bare Metal Nodes for IP addressing
            - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company's discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

VMware System Administration:

Company will support administration of the following base features of VMware ESXi:

- Perform preventative maintenance

Perform emergency maintenance
- Provide performance tuning
- Perform server health checks
- Perform file system maintenance
- Provision Virtual Machines (VM)
- Manage basic vSwitch network
- Manage advanced network switching (i.e. VMware vDS or other vendor supported 3rd party switch)
- Manage basic vStorage network
- Manage VMware server through vCenter
- Manage vCenter application
- Administer built-in VMware dependency components
- Provide utilization reporting

LAN management of the virtual switch is specifically excluded from this scope of Services.

VMware ESXi Triage and Troubleshooting:

- Triage of VMware ESXi incidents
- Troubleshoot and work to resolve VMware ESXi system incidents
- Document VMware ESXi system issues and errors

VMware ESXi Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the ESXi software (including major upgrades) will be conducted at Company's discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into vCenter and general visibility into the Cluster metrics and configuration settings such as as:
    - Cluster and VM performance and analysis
    - Cluster and health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection and recovery policies

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents

- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party ESXi enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AOS is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.
- Client agrees, acknowledges, and understands that the actual manufacture of the VMware ESXi is by VMware, Inc. and its provision and performance may be subject to change as determined by VMware, Inc.
- Client agrees that VMware ESXi offerings provided herein are subject to the VMware Services End User License Agreement available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf and privacy policy located at https://www.vmware.com/help/privacy.html, which are hereby incorporated into this Statement of Work.

602760 ReliaCloud EDGE Node GPC.2407H.E

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

VMware ESXi: VMware's hypervisor platform

Company's Responsibilities and Included Features

ReliaCloud EDGE GPC.2407H.E (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and VMware ESXi. Nodes must minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 5317 (3 GHz, 12 cores), 24 cores total
- 512 GB RAM
- Hybrid performance disk configuration consisting of 24 TB HDD and 7.68 TB SDD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix AOS Ultimate
- Nutanix Prism Pro
- VMware ESXi is not included within this scope, but it is available from Company under a separate ItemID.

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators

Management of iSCSI data services
        - Configure Bare Metal Nodes for IP addressing
            - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company's discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

VMware System Administration:

Company will support administration of the following base features of VMware ESXi:

- Perform preventative maintenance
- Perform emergency maintenance

Provide performance tuning
- Perform server health checks
- Perform file system maintenance
- Provision Virtual Machines (VM)
- Manage basic vSwitch network
- Manage advanced network switching (i.e. VMware vDS or other vendor supported 3rd party switch)
- Manage basic vStorage network
- Manage VMware server through vCenter
- Manage vCenter application
- Administer built-in VMware dependency components
- Provide utilization reporting

LAN management of the virtual switch is specifically excluded from this scope of Services.

VMware ESXi Triage and Troubleshooting:

- Triage of VMware ESXi incidents
- Troubleshoot and work to resolve VMware ESXi system incidents
- Document VMware ESXi system issues and errors

VMware ESXi Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the ESXi software (including major upgrades) will be conducted at Company's discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into vCenter and general visibility into the Cluster metrics and configuration settings such as as:
    - Cluster and VM performance and analysis
    - Cluster and health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection and recovery policies

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the

OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party ESXi enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AOS is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.
- Client agrees, acknowledges, and understands that the actual manufacture of the VMware ESXi is by VMware, Inc. and its provision and performance may be subject to change as determined by VMware, Inc.
- Client agrees that VMware ESXi offerings provided herein are subject to the VMware Services End User License Agreement available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf and privacy policy located at https://www.vmware.com/help/privacy.html, which are hereby incorporated into this Statement of Work.

602765 ReliaCloud EDGE Node HPC.3661N.E

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

VMware ESXi: VMware's hypervisor platform

Company's Responsibilities and Included Features

ReliaCloud EDGE HPC.3661N.E (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and VMware ESXi. Nodes must minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 6353 (3 GHz, 18 cores), 36 cores total
- 1024 GB RAM
- Disk configuration consisting of 61.44TB NVME

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix AOS Ultimate
- Nutanix Prism Pro
- VMware ESXi is not included within this scope, but it is available from Company under a separate ItemID.

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide four (4) network LAN connections that support up to 25 Gbps port speeds

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing

        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company's discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

VMware System Administration:

Company will support administration of the following base features of VMware ESXi:

- Perform preventative maintenance
- Perform emergency maintenance
- Provide performance tuning
- Perform server health checks

Perform file system maintenance
- Provision Virtual Machines (VM)
- Manage basic vSwitch network
- Manage advanced network switching (i.e. VMware vDS or other vendor supported 3rd party switch)
- Manage basic vStorage network
- Manage VMware server through vCenter
- Manage vCenter application
- Administer built-in VMware dependency components
- Provide utilization reporting

LAN management of the virtual switch is specifically excluded from this scope of Services.

VMware ESXi Triage and Troubleshooting:

- Triage of VMware ESXi incidents
- Troubleshoot and work to resolve VMware ESXi system incidents
- Document VMware ESXi system issues and errors

VMware ESXi Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the ESXi software (including major upgrades) will be conducted at Company's discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into vCenter and general visibility into the Cluster metrics and configuration settings such as as:
    - Cluster and VM performance and analysis
    - Cluster and health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection and recovery policies

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party ESXi enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AOS is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.
- Client agrees, acknowledges, and understands that the actual manufacture of the VMware ESXi is by VMware, Inc. and its provision and performance may be subject to change as determined by VMware, Inc.
- Client agrees that VMware ESXi offerings provided herein are subject to the VMware Services End User License Agreement available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf and privacy policy located at https://www.vmware.com/help/privacy.html, which are hereby incorporated into this Statement of Work.

602772 ReliaCloud EDGE Reserved Node GPC.1607H

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Reserved Node GPC.1607H (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- One (1) Intel Xeon-Gold processors 6326 (2.9 GHz, 16 cores), 16 cores total
- 512 GB RAM
- Hybrid performance disk configuration consisting of 24TB HDD and 7.68TB SSD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE Activated Reserved Node Rate (separate Itemd ID), until Client submits a service request for a Reserved Node to be:

  A) Removed from the Cluster, at which point the Reserved Node will remain available and billed (commencing the following month) at its Reserved Node rates;

  or

  B) Elevated to production status, at which point the Reserved Node will become part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node GPC.1607H rate (commencing the following month).

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE Node GPC.1607H Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Activated Reserved Node GPC.1607H Services
- Notify Company to request Node activation, deactivation or changes in use to production status

602774 ReliaCloud EDGE Reserved Node GPC.3215H

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Reserved Node GPC.3215H (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon-Gold processors 6346 (3.1 GHz, 16 cores), 32 cores total
- 1024 GB RAM
- Hybrid performance disk configuration consisting of 48TB HDD and 15.36TB SSD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE Activated Reserved Node Rate (separate Itemd ID), until Client submits a service request for a Reserved Node to be:

A) Removed from the Cluster, at which point the Reserved Node will remain available and billed (commencing the following month) at its Reserved Node rates;

or

B) Elevated to production status, at which point the Reserved Node will become part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node GPC.3215H rate (commencing the following month).

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE Node GPC.3215H Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Activated Reserved Node GPC.3215H Services
- Notify Company to request Node activation, deactivation or changes in use to production status

602775 ReliaCloud EDGE Reserved Node GPC.3230H

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Reserved Node GPC.3230H (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon-Gold processors 6346 (3.1 GHz, 16 cores), 32 cores total
- 1024 GB RAM
- Hybrid performance disk configuration consisting of 64TB HDD and 30.72TB SSD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE Activated Reserved Node Rate (separate Itemd ID), until Client submits a service request for a Reserved Node to be:

  A) Removed from the Cluster, at which point the Reserved Node will remain available and billed (commencing the following month) at its Reserved Node rates;

  or

  B) Elevated to production status, at which point the Reserved Node will become part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node GPC.3230H rate (commencing the following month).

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE Node GPC.3230H Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Activated Reserved Node GPC.3230H Services
- Notify Company to request Node activation, deactivation or changes in use to production status

602776 ReliaCloud EDGE Reserved Node FIL.2415H

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Reserved Node FIL.2415H (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon-Gold processors 5317 (3 GHz, 12 cores), 24 cores total
- 512 GB RAM
- Hybrid performance disk configuration consisting of 120TB HDD and 15.36TB SSD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE Activated Reserved Node Rate (separate Itemd ID), until Client submits a service request for a Reserved Node to be:

  A) Removed from the Cluster, at which point the Reserved Node will remain available and billed (commencing the following month) at its Reserved Node rates;

  or

  B) Elevated to production status, at which point the Reserved Node will become part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node FIL.2415H rate (commencing the following month).

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE Node FIL.2415H Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Activated Reserved Node FIL.2415H Services
- Notify Company to request Node activation, deactivation or changes in use to production status

602788 ReliaCloud EDGE Activated Reserved Node GPC.3230H.A

Company's Responsibilities and Included Features

ReliaCloud EDGE Activated Reserved Node GPC.3230H.A (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. An Activated Node is a ReliaCloud EDGE Reserved Node GPC.3230H that has been joined to an existing Cluster at Client request and is available for Client s use.

A ReliaCloud EDGE Activated Reserved Node is identical to ReliaCloud EDGE Node GPC.3230H.A, except the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company responsibilities, included features, Client responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed in whole month increments for each month that it is activated until Client submits a service request for the Activated Node to be:

A) Removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates (commencing the following month);

or

B) Elevated to production status, at which point the Activated Node will become a part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node GPC.3230H.A rate (commencing the following month).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud EDGE Node GPC.3230H.A Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Reserved Node GPC.3230H Services

602789 ReliaCloud EDGE Activated Reserved Node FIL.2415H.A

Company's Responsibilities and Included Features

ReliaCloud EDGE Activated Reserved Node FIL.2415H.A (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. An Activated Node is a ReliaCloud EDGE Reserved Node FIL.2415H that has been joined to an existing Cluster at Client request and is available for Client s use.

A ReliaCloud EDGE Activated Reserved Node is identical to ReliaCloud EDGE Node FIL.2415H.A, except the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company responsibilities, included features, Client responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed in whole month increments for each month that it is activated until Client submits a service request for the Activated Node to be:

A) Removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates (commencing the following month);

or

B) Elevated to production status, at which point the Activated Node will become a part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node FIL.2415H.A rate (commencing the following month).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

Subscribe to Company s Services for ReliaCloud EDGE Node FIL.2415H.A Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Reserved Node FIL.2415H Services

603841 ReliaCloud BM.6326.32.512

Definitions

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a Cluster, or acts as a stand-alone operating system environment.

Company's Responsibilities and Included Features

ReliaCloud Bare Metal Node BM.6326.32.512 (BM Node) service is comprised of hardware, hosting, and hardware only management services for the node. BM Nodes are designed to support specialized use cases, such as but not limited to:

- Support for software licensing restricted hardware configurations
- Support for ReliaCloud non-standardized hypervisors
- Stand-alone non-virtualized server applications

BM Nodes do not include operating system software, hypervisor software or management. BM Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide a BM Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 6326 (2.9 GHz, 16 cores), 32 cores total
- 512 GB RAM
- BM Node includes no storage. Storage must be delivered via a ReliaCloud storage service contracted under a separate ItemID(s).

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall BM Node solution configuration.

BM Node software specifications:

The BM Node contains no software. Software services may be contracted for under separate ItemIDs.

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the BM Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the BM Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all BM Node physical moves, adds and changes
- Provide up four (4) network LAN connections that support up to 25 Gbps port speeds
- Provide one (1) Out of Band Management LAN connection that supports up to 1 Gbps port speed

BM Node Incident Triage and Troubleshooting:

- Triage of BM Node hardware incidents
- Troubleshooting and work to resolve BM Node hardware incidents
- Document user issues and BM Node hardware related errors
- Management of hardware replacement and/or repair with hardware vendor

Patching, Updates, and Upgrades:

- Periodic reviews of hardware firmware (BIOS) upgrades (Updates)
- Analysis of hardware additions or upgrades
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates will be conducted at Company's discretion and in accordance with industry best practices.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems and or hypervisor support
- Provide software licensing
- Perform all data backup
- Migrate physical machines and/or VMs onto or off of the BM Node

Third Party Utilities and Applications:

- Manage third-party enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

603992 ReliaCloud BM.6334.08.768

Definitions

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a Cluster, or acts as a stand-alone operating system environment.

Company's Responsibilities and Included Features

ReliaCloud Bare Metal Node BM.6334.08.768 (BM Node) service is comprised of hardware, hosting, and hardware only management services for the node. BM Nodes are designed to support specialized use cases, such as but not limited to:

- Support for software licensing restricted hardware configurations
- Support for ReliaCloud non-standardized hypervisors

- Stand-alone non-virtualized server applications

BM Nodes do not include operating system software, hypervisor software or management. BM Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide a BM Node that meets or exceeds the following physical specifications:

- One (1) Intel Xeon Gold processors 6334 (3.6 GHz, 8 cores), 8 cores total
- 768 GB RAM
- BM Node includes no storage. Storage must be delivered via a ReliaCloud storage service contracted under a separate ItemID(s).

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall BM Node solution configuration.

BM Node software specifications:

The BM Node contains no software. Software services may be contracted for under separate ItemIDs.

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the BM Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the BM Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all BM Node physical moves, adds and changes
- Provide up four (4) network LAN connections that support up to 25 Gbps port speeds
- Provide one (1) Out of Band Management LAN connection that supports up to 1 Gbps port speed

BM Node Incident Triage and Troubleshooting:

- Triage of BM Node hardware incidents
- Troubleshooting and work to resolve BM Node hardware incidents
- Document user issues and BM Node hardware related errors
- Management of hardware replacement and/or repair with hardware vendor

Patching, Updates, and Upgrades:

- Periodic reviews of hardware firmware (BIOS) upgrades (Updates)
- Analysis of hardware additions or upgrades
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates will be conducted at Company's discretion and in accordance with industry best practices.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client

staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems and or hypervisor support
- Provide software licensing
- Perform all data backup
- Migrate physical machines and/or VMs onto or off of the BM Node

Third Party Utilities and Applications:

- Manage third-party enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

604143 ReliaCloud EDGE Node 8035r1 - HMAHV

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Node 8035r1 - HMAHV (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE Nodes minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 6226R (2.9 GHz, 16 cores), 32 cores total
- 768 GB RAM
- Hybrid performance disk configuration consisting of 32TB HDD and 15.36TB SSDD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix AOS Ultimate
- Nutanix Prism Pro

Node hosting specifications

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable timeframe based on the severity of the updates, patches or upgrades, Client waives any and all claims against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updates and upgrades are up to date. If patching, updating or upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time updating, patching or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades, updates or patches.

Block and Node Maintenance Management

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable timeframe based on the severity of the update, upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updating and upgrades are up to date. If patching, updating or upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time patching, updating or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for updates, upgrades and/or patches.

Co-administration

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
    - Cluster and VM performance and analysis
    - Cluster and health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection and recovery policies

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request

support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

604368 ReliaCloud Gen 2 Private Cloud Bundle

Company's Responsibilities and Included Features

Provide Client with ReliaCloud private cloud compute and storage utilizing the currently deployed hardware on the Company's ReliaCloud generation 2 (RC2) platform up to the capacity provisioned for Client by Company as of December 1, 2023.

This service is provided at a flat fee per Company location out of which the service is provided with quarterly price escalators as described in the Pricing Notes.

Company will not be liable for any SLA penalties related to the delivery of the RC2 platform.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of any service requirements, changes or modifications
- Operating system and application licensing and supporting maintenance
- Ownership and management of Client applications
- Subscription to Company enterprise firewall services is required
- Subscription to Company provided VMware host server management is required
- Subscription to Company provided VMware software licensing is required
- VPN or WAN connectivity to server through the ReliaCloud network

604684 Legacy Storage Array Usage

Company s Responsibilities and Included Features

Provide Client with storage utilizing the currently deployed Company EMC Clarion or IBM XIV storage arrays as provisioned for Client by Company as of the effective date of this Change Order.

This service is provided at a flat fee per storage array. This fee applies regardless of the amount of storage consumed on the array.

Client may, at Client s expense, migrate the storage off an array and terminate usage of the array at any point in time.

Company will, at Client s direction and expense, explore third parties as additional escalation points in the event of an array failure.

Company will not be liable for any SLA penalties related to the delivery of the storage on these arrays.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client acknowledges and accepts the risks of running systems using storage provided by these arrays, which have ceased to be supported by the original end manufacturer and can fail at any point in time with the additional risk that the arrays and the data may not be recoverable in the case of a failure.

Provide Company with 30 days advanced written notice of intent to discontinue use of a storage array.

604685 ReliaCloud EDGE On-Prem Node FIL.2415H.A

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

File Server Virtual Machine (FSVM): A virtual machine that runs as part of the Nutanix Files file server service.

ICAP: Internet Content Adaptation Protocol (ICAP) is a lightweight protocol designed to offload processing of Internet-based content to dedicated servers. The goal of ICAP, a lightweight HTTP-based RPC protocol, is to offload tasks like antivirus scanning onto specialized servers to increase network throughput.

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Nutanix Files (Files): A software-defined scale-out file storage solution designed to address a wide range of use cases, including but not limited to: support for Linux and Windows home directories, user profiles and department shares.

SMB: Server Message Block, is a network protocol used by Windows-based computers that allows systems within the same

network to share files

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem FIL.2415H.A Node (EDGE Files Node) service is comprised of hardware and a base level of management services for the Nutanix AOS and Nutanix Files Software. EDGE Files Nodes minimally belong to a Cluster configured with at least three (3) EDGE Files Nodes. EDGE Files Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Files Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 5317R (3 GHz, 12 cores), 24 cores total
- 512 GB RAM
- Disk configuration consisting of 15.36 TB SSD
- Disk configuration consisting of 120 TB HDD
- 2x 10/25 Gbps Network Adaptor
- 1x 1GbE Dedicated IPMI

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption as well as the types of workloads that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Files Node that provides a software release that meets or exceeds the following software editions:

- Nutanix Prism Pro

Nutanix AOS and Nutanix Files are licensed seperatley under Company service Nutanix Files License Service - AOS Per TiB.

The EDGE Node includes the following Nutanix software that can be self-enrolled and disenrolled by Customer. Usage of this software may incur additional charges as defined by the Agreement:

- Nutanix Calm Licensing Service - Per VM
- Nutanix Flow Security License Service - Per Node
- Nutanix Objects License Service - AOS Per TiB

AOS Administration:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication

        - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
- Management and Analytics
    - Prism Elements

* Erasure coding is a feature available to Clusters comprised of at least 4 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals. Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

Nutanix Files Administration:

Company will support administration of the following functions:

- File Server Management
    - Creating a file server

        - Maintain the Files Cluster
        - File server cloning
        - Encryption settings
        - Antivirus (AV) scanning (SMB Only)
        - Provide recommendations on File Server Virtual Machines (FSVMs) infrastructure sizing including storage requirements based upon workload.
    - Files Optimization
        - Performance optimization
        - File system compression
    - Share and Export Management
        - Creating file shares
        - Creating exports
        - Multiprotocol support
    - Domain Configuration Management
        - Domain joining
        - Updating Domain Name System (DNS) entries
        - Disjoint domain management
    - Directory and User Management
        - Updating Files directory services
        - Management of user mappings
        - Managing user roles
        - Management of user quotas
    - Data Recovery Management
        - Management of protection domain and snapshot schedule
        - Support for Files asynchronous replication with a minimum 1-hour recovery point objective
        - Upon Client request, activation of disaster recovery of File Server Virtual Machines (FSVMs)
        - Configuration for high availability of FSVMs
        - Configuration of self-service restore (SSR) and snapshot schedule parameters

Nutanix Files analytics is not within scope of this ItemID. Files analytics support is available under a separate ItemID.

Files Triage and Troubleshooting:

- Triage of Files system incidents
- Troubleshoot and work to resolve Files system incidents
- Document Files system issues and error

Nutanix Files analytics is not within scope of this ItemID. Files analytics support is available under a separate ItemID.

Files Patching, Updates and Upgrades:

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of Updates during Company defined maintenance windows
- Periodic upgrades to the Files software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices during Client approved maintenance windows triage of Files system incidents

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
  - Files dashboard
  - File Server alerts and notifications
  - File Server events
- Self-service management
  - Self-service File restoration
  - Execute snapshots and restorations

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client s Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

End of Service Equipment Return

- Company will provide to Client packing materials, prepaid shipping label, and return instructions.
- Professional Services are available for unracking, packing and decommission of equipment under a separate statement of work.
- Company will continue to charge for the supplied On-Prem equipment at the contracted rates until Company takes physical receipt of the assets.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hosting specifications:

Client must complete an environment readiness assessment for Company provided equipment:

- Provide location information of where the EDGE Node will be housed:
  - Address, City, State, Zip
  - On premise contact information Name, email address, phone number
- House the EDGE Node within a power and climate-controlled location that is appropriate for computer and IT storage equipment.

EDGE Node specifications per Node, Client s failure to meet these specifications will excuse Company from availability SLAs:

Min Cluster Size	3 Nodes
Power Ranges Per Node	822W Typical 1175W maximum
Power Delivery	Continuous feeds 2x 208V 20 Amp
Operating Requirements	Input Voltage: 100-240V AC auto-range, Input Frequency: 50-60Hz
Power Diversity	A & B UPS + Backup Power (generator)
Operating Environment	Op Temp Range: 50 to 95 F (10 to 35 C) Op Humidity Range (non-condensing): 68 to 194 F (20 to 90 C)
Rough Dimensions Per Node	Height: 3.47" Width: 17.36" Depth: 29.18" Rack Units: 2U
Network Connections Per Node	2 x 25 Gbps SFP 1 x 1 GbE (TX)

- The Service Level Objective (SLO) for repair or replacement is next business day or better.
- Provide a secure cabinet or other approved Company enclosure to house EDGE Node
- Maintain environmental standards for HVAC consistent with primary hosting facility.
- Maintain physical security of the cabinet.
- Connect the Network Switch48 to Client s network core if applicable.
- Open any necessary firewall or network ports and conduits to allow a connection between the EDGE Node and the Company s network operation center.
- Assist with any physical interaction for EDGE Node repair or replacement as needed, and provide escorted access to the EDGE Node for Company and/or Company s authorized service vendor.
- Coordinate all Client responsibilities outlined herein, including all necessary communication to Client personnel.
- Provide or purchase all necessary equipment, cabling, circuits, and other materials required for the services, unless OneNeck explicitly provides that such materials are included as part of the services.
- Ensure compliance with any national or local safety standard or similar requirement affecting the installation of the EDGE Node.
- Provide Company with access, passwords, access codes or security devices as necessary to perform the services.

End of Service Equipment Return

Upon termination of this service, Client must return the equipment in good working condition to Company. The procedure to initiate equipment returns is to create a ticket with the Company Service Desk. This can be conducted via phone, email, or web portal. Additional activities include:

- Unrack, remove cables, and pack Company s provided equipment into Company s provided return shipping materials.
- Coordinate transfer of equipment to Company s specified courier.

- Ship all devices to OneNeck within five (5) business days after receipt of Company s provided packing materials.
- Equipment not returned within a timely fashion will be billed at existing company s rates, until receipt.

General Requirements

- Own and manage guest VM applications and operating systems support
- Subscribe to Company Nutanix Files License Service - AOS Per TiB.
- Manage end user Files share access management and usage
- For anti-virus scanning support, provide ICAP compatible anti-virus software
- Migration of Files data onto and off of the Cluster
- Open necessary network and firewall ports to provide Company access to Management VMs
- Provide VPN termination point for Company to access Client s environment
- Perform all data backup
- Provide Company with a snapshot policy
- Execute file level self-service restorations
- Provide a directory service and credentials to integrate into the file servicePerform all data backup
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment
- This platform includes software features that are Customer discoverable and allow for self-enrollment. These services are metered usage and will bill monthly based upon their usage. The following ItemIDs must be subscribed to, but don't require their use unless desired by Customer:
  - 606609 Nutanix Calm Licensing Service - Per VM
  - 606610 Nutanix Flow Security License Service - Per Node
  - 606611 Nutanix Files License Service - AOS Per TiB
  - 606612 Nutanix Objects License Service - AOS Per TiB
- Subscribe to Company Remote Management Infrastructure (1-24 devices) service, ItemID 500159

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are solely Client s responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to, and governed by, the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full

604686 ReliaCloud EDGE On-Prem Reserved Node FIL.2415H.A

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Reserved Node FIL.2415H (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon-Gold processors 5317 (3 GHz, 12 cores), 24 cores total
- 512 GB RAM
- Hybrid performance disk configuration consisting of 120TB HDD and 15.36TB SSD

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE Activated Reserved Node Rate (separate Itemd ID), until Client submits a service request for a Reserved Node to be:

A) Removed from the Cluster, at which point the Reserved Node will remain available and billed (commencing the following month) at its Reserved Node rates;

or

B) Elevated to production status, at which point the Reserved Node will become part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node FIL.2415H rate (commencing the following month).

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE Node FIL.2415H Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Activated Reserved Node FIL.2415H Services
- Notify Company to request Node activation, deactivation or changes in use to production status

604687 ReliaCloud EDGE On-Prem Reserved Activated Node FIL.2415H.A

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Activated Reserved Node FIL.2415H.A (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. An Activated Node is a ReliaCloud EDGE On-Prem Reserved Node FIL.2415H.A that has been joined to an existing Cluster at Client request and is available for Client s use.

A ReliaCloud EDGE On-Prem Activated Reserved Node is identical to ReliaCloud EDGE On-Prem Node FIL.2415H.A, except the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company responsibilities, included features, Client responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed monthly in whole day increments for each day that it is activated until Client submits a service request for the Activated Node to be:

A) Removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates.

or

B) Elevated to production status, at which point the Activated Node will become a part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE On-Prem Node FIL.2415H.A rate.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud EDGE On-Prem Node FIL.2415H.A Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE On-Prem Reserved Node FIL.2415H.A Services

606631 ReliaCloud On-Prem Network Switch - 48 Ports

Definitions

HCI : Hyperconverged infrastructure. A cloud virtualization architecture that creates Clusters from Nodes.

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud On-Prem Network Switch - 48 Ports (Switch48) provides a managed physical network switch to connect HCI infrastructure and other associated IT infrastructure components, such as but not limited to firewalls, WAN routers, and other supporting appliances. Switch48 is designed to provide up to 48 physical connections. Switch48 is a building block component to serve a number of deployment solutions, i.e., two (2) Switch48s would be required to create a high-available network design.

Intended use. The intent of this infrastructure is to provide an adequate and performant network solution to interconnect the ReliaCloud EDGE Nodes, that are part of the overall solution. Solution is intended to interconnect to a larger Client s LAN network via uplink connections. Use outside of this purpose requires Company s approval.

Infrastructure physical specifications:

Company will provide network infrastructure that meets or exceeds the following physical specifications:

- One (1) switch with the following specifications
  - 48 Ports consisting capable of 1 / 10 / 25 Gbps speed
  - Typical power output of up to 325W, maximum power output of 600W
  - 1 RU of cabinet space
  - Switch48 will typically consume two (2) uplink network ports to Client infrastructure
- Company at its choosing, may also require space, power, and connectivity for an out of band serial connection appliance to support the Switch48.
  - 2x RJ45 1GbE ports
  - Sub 1 RU of cabinet space

Switch48 is a fixed configuration model. Desired capacity consumption above the 48 ports may require a complete architectural change and contract adjustment and would be at Company s discretion. Port consumption is typically expected to be 2 connections per Node for network traffic, and 1 connection to the Node s IPMI (IP management interface) port. For High availability solutions, the port connections should be distributed across two (2) Switch48s.

All port usage by Client must be approved by Company. This process can be accomplished by opening a ticket with Company s service desk. Switch48 service requires that Internet services are available to the environment by the Client. Internet Service will be leveraged to create an encrypted services tunnel to the Company s Network Operations Center (NOC) for management operations and metered billing services. The connection speeds are expected to be at least 10 mbps.

Network Administration:

- For any Layer 2 extension
  - No spanning tree
  - Port channel with LACP required
- Optics
  - DAC cables (cabinet design)
  - Cisco Optics
- Support for VRFs
  - DMZ VRF
  - Port channel management
  - Interface management
- Layer 2
  - VLAN MACs
  - VLAN trunk management
- Layer 3
  - Basic IP configuration
  - Static routes MACs
  - BGP
  - Provide cables between Company equipment and Device
  - Provide small form-factor pluggable transceivers (SFP s) for Company s side of the connection
  - Service is Layer 2
  - VLAN configuration activities, including provisions of secure VLAN trunks
  - Upon Client s written request, service supports port-channel / link-aggregation configuration using Link Aggregation Control Protocol (LACP) or static configuration

Network Stack Incident Triage and Troubleshooting:

- Triage of network stack hardware or operating system incidents

- Troubleshooting and work to resolve hardware or operating system incidents
- Document user issues and system errors

Network Stack Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the Network Stack software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Co-administration:

Company does not allow co-administration on the Switch48, except for emergency on-premises troubleshooting via temporary administration privileges, granted by Company. Read-only SNMP access can be provided upon Client s written request.

Expert User Technical Support:

Technical support may only be requested by a Client s Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

End of Service Equipment Return

- Company will provide to Client packing materials, prepaid shipping label, and return instructions.
- Professional Services are available for unracking, packing and decommission of equipment under a separate statement of work.
- Company will continue to charge for the supplied On-Prem equipment at the contracted rates until Company takes physical receipt of the assets.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hosting specifications:

Client must complete an environment readiness assessment for Company provided equipment:

- Provide location information of where the EDGE Node will be housed:
  - Address, City, State, Zip
  - On premise contact information Name, email address, phone number
- House the Switch48 and if provided Out of Band Serial Appliance within a power and climate-controlled location that is appropriate for computer and IT storage equipment.

Device	Network Switch 48 Ports
Power Ranges	260W Typical 425W maximum
Power Delivery	Continuous feeds 2x 100-240V
Operating Requirements	Input Voltage: 100-240V AC auto-range, Input Frequency: 50-60Hz
Power Diversity	A & B UPS + Backup Power (generator)
Operating Environment	Op Temp Range: 32 to 104 F Op Humidity Range 5 to 95% (non-condensing):
Rough Dimensions Per Node	Height: 1.72" Width: 17.3" Depth: 22.5" Rack Units: 1RU
Network Connections Per Node	2 x 25 Gbps SFP 1 x 1 GbE (TX)

Device	Out of Band Serial Appliance
Power Ranges	5W to 15W typical
Power Delivery	7-20 VDC power input, 2V 3A power supply included (with twist lock)
Operating Requirements	Input Voltage: 100-240V AC auto-range, Input Frequency: 50-60Hz
Power Diversity	None Single power connection
Operating Environment	Operation: (-4 to 140 F), 5-95% RH, non-cond.
Rough Dimensions Per Node	Height: 1.34" Width: 3.3" Depth: 4.4" Rack Units: 0RU
Network Connections Per Node	2x Gigabit (10/100/1000BT) Ethernet interfaces on RJ45

- Provide a secure cabinet or other approved Company s enclosure to house the Switch48.
- Maintain physical security of the cabinet.
- Connect the Network Switch48 to Client s network core if applicable.
- Open any necessary firewall or network ports and conduits to allow a connection between the Switch48 and Out of Band Serial Appliance to the Company s network operation center.
- Assist with any physical interaction for Switch48 repair or replacement as needed, and provide escorted access to the Switch48 for Company and/or Company s authorized service vendor.
- Coordinate all Client s responsibilities outlined herein, including all necessary communication to Client s personnel.
- Provide or purchase all necessary equipment, cabling, circuits, and other materials required for the services, unless OneNeck explicitly provides that such materials are included as part of the services.
- Ensure compliance with any national or local safety standard or similar requirement affecting the installation of the Switch48.
- Provide Company with access, passwords, access codes or security devices as necessary to perform the services.

End of Service Equipment Return

Upon termination of this service, Client must return the equipment in good working condition to Company. The procedure to

initiate equipment returns is to create a ticket with the Company Service Desk. This can be conducted via phone, email, or web portal. Additional activities include:

- Unrack, remove cables, and pack Company s provided equipment into Company s provided return shipping materials.
- Coordinate transfer of equipment to Company s specified courier.
- Ship all devices to OneNeck within five (5) business days after receipt of Company s provided packing materials.
- Equipment not returned within a timely fashion will be billed at existing company s rates, until receipt.

General Requirements

- Maintain a subscription to ReliaCloud EDGE On-Prem Nodes in the location where the Network Switch48 resides

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are solely Client s responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to, and governed by, the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full

606856 ReliaCloud Gen 2 Private Cloud Bundle

Company's Responsibilities and Included Features

Provide Client with ReliaCloud private cloud compute and storage utilizing the currently deployed hardware on the Company's ReliaCloud generation 2 (RC2) platform up to the capacity provisioned for Client by Company as of December 1, 2023.

This service is provided at a flat fee per Company location out of which the service is provided with quarterly price escalators as described in the Pricing Notes.

Company will not be liable for any SLA penalties related to the delivery of the RC2 platform.

The service is being offered specific to (4) virtual machines that are specifically dedicated to supporting Client s ShoreTel voice system. No additional workloads may be added to the ReliaCloud Gen 2 Private Cloud Bundle, nor may any workloads/VMs be expanded.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of any service requirements, changes or modifications
- Operating system and application licensing and supporting maintenance
- Ownership and management of Client applications
- Subscription to Company enterprise firewall services is required
- Subscription to Company provided VMware host server management is required
- Subscription to Company provided VMware software licensing is required
- VPN or WAN connectivity to server through the ReliaCloud network

610928 ReliaCloud EDGE On-Prem Node HPC.7269F.E

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

VMware ESXi: VMware's hypervisor platform

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Node HPC.7269F.E (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and VMware ESXi. EDGE Nodes minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- 4 x Intel Xeon-Gold 6254 processors (3.1 GHz/ 18-core/ 230W) (72 Cores)
- 3072 GB RAM
- Disk configuration consisting of 61.44TB SSD
- Disk configuration consisting of 15.36TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI (Nutanix Cloud Infrastructure) Ultimate

- Nutanix NCM (Nutanix Cloud Manager) Pro
- VMware ESXi is not included within this scope, but it is available from Company under a separate ItemID.

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)

Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node maintenance management is limited to:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

VMware System Administration:

Company will support administration of the following base features of VMware ESXi:

- Perform preventative maintenance
- Perform emergency maintenance
- Provide performance tuning
- Perform server health checks
- Perform file system maintenance
- Provision Virtual Machines (VM)
- Manage basic vSwitch network
- Manage advanced network switching (i.e. VMware vDS or other vendor supported 3rd party switch)
- Manage basic vStorage network
- Manage VMware server through vCenter
- Manage vCenter application
- Administer built-in VMware dependency components
- Provide utilization reporting

LAN management of the virtual switch is specifically excluded from this scope of Services.

VMware ESXi Triage and Troubleshooting:

- Triage of VMware ESXi incidents
- Troubleshoot and work to resolve VMware ESXi system incidents
- Document VMware ESXi system issues and errors

VMware ESXi Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates

Application of Updates during Company defined maintenance windows

- Periodic application of the Updates to the ESXi software (including major upgrades) will be conducted at Company's discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features are available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
  - Cluster and VM performance and analysis
  - Cluster, health and availability
  - Cluster capacity and trend info
  - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
  - Create, delete and modify VMs
  - Execute snapshots and restorations
  - Add VMs to catalog
  - Import, add, create and delete images to catalog
  - Create and modify data protection and recovery policies

Upon Client s written request, Company will provide account(s) with administrator level and or viewer privileges.

Company s SLA obligations will not apply to incidents caused by Client s co-administration activities. Company s remediation of Client s caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client s Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

End of Service Equipment Return

- Company will provide to Client packing materials, prepaid shipping label, and return instructions.
- Professional Services are available for unracking, packing and decommission of equipment under a separate statement of work.
- Company will continue to charge for the supplied On-Prem equipment at the contracted rates until Company takes physical receipt of the assets.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hosting specifications:

Client must complete an environment readiness assessment for Company provided equipment:

- Provide location information of where the EDGE Node will be housed:
  - Address, City, State, Zip
  - On premise contact information Name, email address, phone number
- House the EDGE Node within a power and climate-controlled location that is appropriate for computer and IT storage equipment as specified in the table below.

EDGE Node specifications per Node, Client s failure to meet these specifications will excuse Company from availability SLAs:

Min Cluster Size	3 Nodes
Power Ranges Per Node	940W Typical 2200W maximum
Power Delivery	Continuous feeds 2x 208V 20 Amp
Operating Requirements	Input Voltage: 100-240V AC auto-range, Input Frequency: 50-60Hz
Power Diversity	A & B UPS + Backup Power (generator)
Operating Environment	Op Temp Range: 50 to 95 F (10 to 35 C) 8% to 90% relative humidity (Rh), 28 C (82.4 F) maximum wet bulb temperature, non-condensing
Rough Dimensions Per Node	Height: 3.44" Width: 17.54" Depth: 29.71" Rack Units: 2RU
Network Connections Per Node	2 x 25 Gbps SFP 1 x 1 GbE (TX)

- The Service Level Objective (SLO) for repair or replacement is next business day or better.
- Provide a secure cabinet or other enclosure to house EDGE Node
- Maintain environmental standards for HVAC consistent with primary hosting facility.
- Maintain physical security of the cabinet.
- Connect the Network Switch48 to Client s network core if applicable.
- Open any necessary firewall or network ports and conduits to allow a connection between the EDGE Node and the Company s network operation center.
- Assist with any physical interaction for EDGE Node repair or replacement as needed, and provide escorted access to the EDGE Node for Company and/or Company s authorized service vendor.
- Coordinate all Client responsibilities outlined herein, including all necessary communication to Client personnel.
- Provide or purchase all necessary equipment, cabling, circuits, and other materials required for the services, unless OneNeck explicitly provides that such materials are included as part of the services.
- Ensure compliance with any national or local safety standard or similar requirement affecting the installation of the EDGE Node.

- Provide Company with access, passwords, access codes or security devices as necessary to perform the services.

End of Service Equipment Return

Upon termination of this service, Client must return the equipment in good working condition to Company. The procedure to initiate equipment returns is to create a ticket with the Company Service Desk. This can be conducted via phone, email, or web portal. Additional activities include:

- Unrack, remove cables, and pack Company s provided equipment into Company s provided return shipping materials.
- Coordinate transfer of equipment to Company s specified courier.
- Ship all devices to OneNeck within five (5) business days after receipt of Company s provided packing materials.
- Equipment not returned within five (5) business days after receipt of Company s provided packing materials will be billed at existing company s rates, until received by Company s specified courier.

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment
- Subscribe to Company Remote Management Infrastructure (1-24 devices) service, ItemID 500159

Third Party Utilities and Applications:

- Manage third-party ESXi enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are solely Client s responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees that Nutanix offerings provided herein are subject to, and governed by, the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full
- Client agrees, acknowledges, and understands that the actual manufacture of the VMware ESXi is by VMware, Inc. and its provision and performance may be subject to change as determined by VMware, Inc.
- Client agrees that VMware ESXi offerings provided herein are subject to the VMware Services End User License Agreement available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf and privacy policy located at https://www.vmware.com/help/privacy.html, which are hereby incorporated into this Statement of Work.

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Reserved Node HPC.7269F.E (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- 4 x Intel Xeon-Gold 6254 processors (3.1 GHz/ 18-core/ 230W) (72 Cores)
- 3072 GB RAM
- Disk configuration consisting of 61.44TB SSD
- Disk configuration consisting of 15.36TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE On-Prem Activated Reserved Node Rate, until Client submits a service request for a Reserved Node to be removed from the Cluster, at which point the Reserved Node will remain available and billed at its Reserved Note rates.

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE On-Prem Node HPC.7269F.E Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud On-Prem EDGE Activated Reserved Node HPC.7269F.E Services
- Notify Company to request Node activation, deactivation or changes in use to production status

610930 ReliaCloud EDGE On-Prem Activated Reserved Node HPC.7269F.E

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Activated Reserved Node HPC.7269F.E (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and VMware ESXi. An Activated Node is a ReliaCloud EDGE On-Prem Reserved Node HPC.7269F.E that has been joined to an existing Cluster at Client request and is available for Client s use.

A ReliaCloud EDGE On-Prem Activated Reserved Node is identical to ReliaCloud EDGE On-Prem Node HPC.7269F.E, except the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company responsibilities, included features, Client responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed monthly in whole day increments for each day that it is activated until Client submits a service request for the Activated Node to be:

A) Removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates.

or

B) Elevated to production status, at which point the Activated Node will become a part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE On-Prem Node HPC.7269F.E rate.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud EDGE On-Prem Node HPC.7269F.E Services and have a Cluster of at least three (3) Nodes

- Subscribe to Company s ReliaCloud EDGE On-Prem Reserved Node HPC.7269F.E Services

611099 ReliaCloud EDGE Node GPC.1630N.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Node GPC 1630N.A (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE Nodes minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Intel processor(s), 16 cores total
- 512 GB RAM
- Disk configuration consisting of 30.72 TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI (Nutanix Cloud Infrastructure) Ultimate
- Nutanix NCM (Nutanix Cloud Manager) Pro

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding (EC-X) is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription

- Periodic reviews of critical patches

Block and Node Maintenance Management:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
  - Virtual Machine (VM) centric snapshots and clones
  - VM-centric Storage QoS
  - VM Flash Mode
- Data Protection
  - Application consistent snapshots
  - Local snapshots
  - Self-service restores
  - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
  - VM management. VM s operating system management and application management is specifically excluded from this scope.
  - VM automated resource scheduling
  - VM affinity rules
  - Virtual network configuration
  - Host profiles
  - VM high availability
  - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client includes:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
  - Cluster and VM performance and analysis
  - Cluster and health and availability
  - Cluster capacity and trend info
  - Alerts and notifications

- Creation of customized dashboards
- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection and recovery policies

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company's SLA obligations will not apply to incidents caused by Client co-administration activities. Company's remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.

- Client agrees that Nutanix's offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

611100 ReliaCloud EDGE Reserved Node GPC.1630N

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Reserved Node GPC.1630N (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Intel processor(s), 16 cores total
- 512 GB RAM
- Disk configuration consisting of 30.72 TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including, but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE Activated Reserved Node Rate (separate Item ID), until Client submits a service request for a Reserved Node to be:

  A) Removed from the Cluster, at which point the Reserved Node will remain available and billed (commencing the following month) at its Reserved Node rates;

  or

  B) Elevated to production status, at which point the Reserved Node will become part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node GPC.1630N rate (commencing the following month).

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE Node GPC.1630N Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Activated Reserved Node GPC.1630N Services
- Notify Company to request Node activation, deactivation or changes in use to production status

611101 ReliaCloud EDGE Activated Reserved Node GPC.1630N.A

Company's Responsibilities and Included Features

ReliaCloud EDGE Activated Reserved Node GPC.1630N.A (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. An Activated Node is a ReliaCloud EDGE Reserved Node GPC.1630N that has been joined to an existing Cluster at Client's request and is available for Client s use.

A ReliaCloud EDGE Activated Reserved Node is identical to ReliaCloud EDGE Node GPC.1630N.A, except for the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company's responsibilities, included features, Client responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed in whole month increments for each month that it is activated until Client submits a service request for the Activated Node to be:

A) Removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates (commencing the following month);

or

B) Elevated to production status, at which point the Activated Node will become a part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node GPC.1630N.A rate (commencing the following month).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud EDGE Node GPC.1630N.A Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Reserved Node GPC.1630N Services

611102 ReliaCloud EDGE Node GPC.1630N.E

Definitions

AOS: Nutanix Acropolis Operating System is a Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

VMware ESXi: VMware's hypervisor platform

Company's Responsibilities and Included Features

ReliaCloud EDGE GPC.1630N.E (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and VMware ESXi. Nodes must minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

Intel processor(s), 16 cores total
- 512 GB RAM
- Disk configuration consisting of 30.72 TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including, but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI (Nutanix Cloud Infrastructure) Ultimate
- Nutanix NCM (Nutanix Cloud Manager) Pro
- VMware ESXi is not included within this scope, but it is available from Company under a separate ItemID.

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - Configuration and management of Challenge-Handshake Authentication (CHAP) if Company determines it as a requirement
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)

- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company's discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

VMware System Administration:

Company will support administration of the following base features of VMware ESXi:

- Perform preventative maintenance
- Perform emergency maintenance
- Provide performance tuning
- Perform server health checks
- Perform file system maintenance
- Provision Virtual Machines (VM)
- Manage basic vSwitch network
- Manage advanced network switching (i.e. VMware vDS or other vendor supported 3rd party switch)
- Manage basic vStorage network
- Manage VMware server through vCenter
- Manage vCenter application
- Administer built-in VMware dependency components
- Provide utilization reporting

LAN management of the virtual switch is specifically excluded from this scope of Services.

VMware ESXi Triage and Troubleshooting:

- Triage of VMware ESXi incidents
- Troubleshoot and work to resolve VMware ESXi system incidents
- Document VMware ESXi system issues and errors

VMware ESXi Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the ESXi software (including major upgrades) will be conducted at Company's discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into vCenter and general visibility into the Cluster metrics and configuration settings, such as as:
    - Cluster and VM performance and analysis
    - Cluster and health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection and recovery policies

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems support
- Perform all data backup

Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party ESXi enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client's business continuity plan(s) and disaster recovery plan(s) are Client's responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AOS is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.
- Client agrees, acknowledges, and understands that the actual manufacture of the VMware ESXi is by VMware, Inc. and its provision and performance may be subject to change as determined by VMware, Inc.
- Client agrees that VMware ESXi offerings provided herein are subject to the VMware Services End User License Agreement available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf and privacy policy located at https://www.vmware.com/help/privacy.html, which are hereby incorporated into this Statement of Work.

611103 ReliaCloud EDGE Activated Reserved Node GPC.1630N.E

Company's Responsibilities and Included Features

ReliaCloud EDGE Activated Reserved Node GPC.1630N.E (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and VMWare ESXi. An Activated Node is a ReliaCloud EDGE Reserved Node GPC.1630N that has been joined to an existing Cluster at Client s request and is available for Client s use.

A ReliaCloud EDGE Activated Reserved Node is identical to ReliaCloud EDGE Node GPC.1630N.E, except for the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company s responsibilities, included features, Client s responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed in whole month increments for each month that it is activated until Client submits a service request for the Activated Node to be:

A) Removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates (commencing the following month);

or

B) Elevated to production status, at which point the Activated Node will become a part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node GPC.1630N.E rate (commencing the following month).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud EDGE Node GPC.1630N.E Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Reserved Node GPC.1630N Services

611104 ReliaCloud EDGE Node GPC.3292N.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Node GPC 3292N.A (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE Nodes minimally belonging to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Intel processor(s), 32 cores total
- 1024 GB RAM
- Disk configuration consisting of 92.16 TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity, including but not limited to the Cluster s Node failure resiliency design, storage configuration settings, such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI (Nutanix Cloud Infrastructure) Ultimate
- Nutanix NCM (Nutanix Cloud Manager) Pro

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding (EC-X) is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, includes:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
    - Cluster and VM performance and analysis

        - Cluster and health and availability
        - Cluster capacity and trend info
        - Alerts and notifications
    - Creation of customized dashboards
    - Self-service management of virtual infrastructure
        - Create, delete and modify VMs
        - Execute snapshots and restorations
        - Add VMs to catalog
        - Import, add, create and delete images to catalog
        - Create and modify data protection and recovery policies

Upon Client s request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.

- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

611105 ReliaCloud EDGE Reserved Node GPC.3292N

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Reserved Node GPC.3292N (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Intel processor(s), 32 cores total
- 1024 GB RAM
- Disk configuration consisting of 92.16 TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity, including but not limited to the Cluster s Node failure resiliency design, storage configurations settings, such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE Activated Reserved Node Rate (separate Item ID), until Client submits a service request for a Reserved Node to be:

  A) Removed from the Cluster, at which point the Reserved Node will remain available and billed (commencing the following month) at its Reserved Node rates;

  or

  B) Elevated to production status, at which point the Reserved Node will become part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node GPC.3292N rate (commencing the following month).

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client s request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE Node GPC.3292N Services and have a Cluster of at least three (3) Nodes

- Subscribe to Company s ReliaCloud EDGE Activated Reserved Node GPC.3292N Services
- Notify Company to request Node activation, deactivation or changes in use to production status

611106 ReliaCloud EDGE Activated Reserved Node GPC.3292N.A

Company's Responsibilities and Included Features

ReliaCloud EDGE Activated Reserved Node GPC.3292N.A (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. An Activated Node is a ReliaCloud EDGE Reserved Node GPC.3292N that has been joined to an existing Cluster at Client s request, and is available for Client s use.

A ReliaCloud EDGE Activated Reserved Node is identical to ReliaCloud EDGE Node GPC.3292N.A, except for the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company s responsibilities, included features, Client responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed in whole month increments for each month that it is activated until Client submits a service request for the Activated Node to be:

A) Removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates (commencing the following month);

or

B) Elevated to production status, at which point the Activated Node will become a part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node GPC.3292N.A rate (commencing the following month).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud EDGE Node GPC.3292N.A Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Reserved Node GPC.3292N Services

611107 ReliaCloud EDGE Node GPC.3292N.E

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

VMware ESXi: VMware's hypervisor platform

Company's Responsibilities and Included Features

ReliaCloud EDGE GPC.3292N.E (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and VMware ESXi. Nodes must minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Intel processor(s), 32 cores total
- 1024 GB RAM
- Disk configuration consisting of 92.16 TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings, such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI (Nutanix Cloud Infrastructure) Ultimate
- Nutanix NCM (Nutanix Cloud Manager) Pro
- VMware ESXi is not included within this scope, but it is available from Company under a separate ItemID.

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication

        - Cluster lockdown
        - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding (EC-X) is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company's discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

VMware System Administration:

Company will support administration of the following base features of VMware ESXi:

- Perform preventative maintenance
- Perform emergency maintenance
- Provide performance tuning
- Perform server health checks
- Perform file system maintenance
- Provision Virtual Machines (VM)
- Manage basic vSwitch network
- Manage advanced network switching (i.e. VMware vDS or other vendor supported 3rd party switch)
- Manage basic vStorage network
- Manage VMware server through vCenter
- Manage vCenter application

Administer built-in VMware dependency components
- Provide utilization reporting

LAN management of the virtual switch is specifically excluded from this scope of Services.

VMware ESXi Triage and Troubleshooting:

- Triage of VMware ESXi incidents
- Troubleshoot and work to resolve VMware ESXi system incidents
- Document VMware ESXi system issues and errors

VMware ESXi Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the ESXi software (including major upgrades) will be conducted at Company's discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, includes:

- Ability to login into vCenter and general visibility into the Cluster metrics and configuration settings such as:
  - Cluster and VM performance and analysis
  - Cluster and health and availability
  - Cluster capacity and trend info
  - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
  - Create, delete and modify VMs
  - Execute snapshots and restorations
  - Add VMs to catalog
  - Import, add, create and delete images to catalog
  - Create and modify data protection and recovery policies

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company s SLA obligations will not apply to incidents caused by Client s co-administration activities. Company s remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party ESXi enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client s responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AOS is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.
- Client agrees, acknowledges, and understands that the actual manufacture of the VMware ESXi is by VMware, Inc. and its provision and performance may be subject to change as determined by VMware, Inc.
- Client agrees that VMware ESXi offerings provided herein are subject to the VMware Services End User License Agreement available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf and privacy policy located at https://www.vmware.com/help/privacy.html, which are hereby incorporated into this Statement of Work.

611108 ReliaCloud EDGE Activated Reserved Node GPC.3292N.E

Company's Responsibilities and Included Features

ReliaCloud EDGE Activated Reserved Node GPC.3292N.E (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and VMWare ESXi. An Activated Node is a ReliaCloud EDGE Reserved Node GPC.3292N that has been joined to an existing Cluster at Client s request and is available for Client s use.

A ReliaCloud EDGE Activated Reserved Node is identical to ReliaCloud EDGE Node GPC.3292N.E, except for the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company s responsibilities, included features, Client s responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed in whole month increments for each month that it is activated until Client submits a service request for the Activated Node to be:

A) Removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates (commencing the following month);

or

B) Elevated to production status, at which point the Activated Node will become a part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node GPC.3292N.E rate (commencing the following month).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud EDGE Node GPC.3292N.E Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Reserved Node GPC.3292N Services

611109 ReliaCloud EDGE Node GPC.4892N.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Node GPC 4892N.A (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE Nodes minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Intel processor(s), 48 cores total
- 1024 GB RAM
- Disk configuration consisting of 92.16 TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity, including but not limited to the Cluster s Node failure resiliency design, storage configuration settings, such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI (Nutanix Cloud Infrastructure) Ultimate
- Nutanix NCM (Nutanix Cloud Manager) Pro

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet

Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
  - Cluster sizing including heterogeneous Clusters
  - Data tiering
  - Inline compression
  - Inline performance deduplication
  - Online Cluster growth
  - Compression
  - Deduplication
  - Erasure coding (EC-X) *
- Nutanix Volumes Management
  - Creation of iSCSI volume group(s)
  - Management of volume groups
  - Management of client iSCSI initiators
  - Management of iSCSI data services
  - Configure Bare Metal Nodes for IP addressing
    - Configuration and management of Challenge-Handshake Authentication (CHAP), if Company determines it as a requirement
- Infrastructure Resilience
  - Data path redundancy
  - Tunable redundancy factor
- Security
  - Client authentication
  - Cluster lockdown
  - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
  - Prism Central and Prism Elements
  - Pulse
  - Cluster health

* Erasure coding (EC-X) is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
  - Virtual Machine (VM) centric snapshots and clones
  - VM-centric Storage QoS
  - VM Flash Mode
- Data Protection
  - Application consistent snapshots
  - Local snapshots
  - Self-service restores
  - Asynchronous replication with a minimum of 1-hour recovery point objective (RPO)
- Virtualization Features
  - VM management. VM s operating system management and application management is specifically excluded from this scope.
  - VM automated resource scheduling
  - VM affinity rules
  - Virtual network configuration
  - Host profiles
  - VM high availability
  - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service

features available to Client, includes:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
  - Cluster and VM performance and analysis
  - Cluster and health and availability
  - Cluster capacity and trend info
  - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
  - Create, delete and modify VMs
  - Execute snapshots and restorations
  - Add VMs to catalog
  - Import, add, create and delete images to catalog
  - Create and modify data protection and recovery policies

Upon Client s request, Company will provide account(s) with administrator level and/or viewer privileges.

Company s SLA obligations will not apply to incidents caused by Client s co-administration activities. Company s remediation of Client s caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priorities 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priorities 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client, as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client s business continuity plan(s) and disaster recovery plan(s) are Client s responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.

- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

611110 ReliaCloud EDGE Node GPC.48153N.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is a Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Node GPC 48153N.A (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE Nodes minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Intel processor(s), 48 cores total
- 2048 GB RAM
- Disk configuration consisting of 153.6 TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity, including but not limited to the Cluster s Node failure resiliency design, storage configuration settings, such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI (Nutanix Cloud Infrastructure) Ultimate
- Nutanix NCM (Nutanix Cloud Manager) Pro

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - Configuration and management of Challenge-Handshake Authentication (CHAP), if Company determines it as a requirement
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding (EC-X) is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client s notification of Updates
- Application of Updates during Company s defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes

Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum of 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client s notification of Updates
- Application of Updates during Company s defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, includes:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
    - Cluster and VM performance and analysis
    - Cluster and health and availability

        - Cluster capacity and trend info
        - Alerts and notifications
    - Creation of customized dashboards
    - Self-service management of virtual infrastructure
        - Create, delete and modify VMs
        - Execute snapshots and restorations
        - Add VMs to catalog
        - Import, add, create and delete images to catalog
        - Create and modify data protection and recovery policies

Upon Client s request, Company will provide account(s) with administrator level and/or viewer privileges.

Company s SLA obligations will not apply to incidents caused by Client s co-administration activities. Company s remediation of Client s caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client s Expert User*, available during the following hours:

- 24 x 7 technical support for priorities 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priorities 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client, as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client s business continuity plan(s) and disaster recovery plan(s) are Client s responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.

- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

611111 ReliaCloud EDGE Reserved Node GPC.4892N

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Reserved Node GPC.4892N (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Intel processor(s), 48 cores total
- 1024 GB RAM
- Disk configuration consisting of 92.16 TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity, including but not limited to the Cluster s Node failure resiliency design, storage configurations settings, such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE Activated Reserved Node Rate (separate Item ID), until Client submits a service request for a Reserved Node to be:

  A) Removed from the Cluster, at which point the Reserved Node will remain available and billed (commencing the following month) at its Reserved Node rates;

  or

  B) Elevated to production status, at which point the Reserved Node will become part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node GPC.4892N rate (commencing the following month).

Service Level Objective (SLO)

- The SLO for Company s delivery of a Dedicated Reserved Node to an activated state, from the time of Client s request to visibility within Prism Central, is eight (8) hours. This SLO is subject to the SLA service availability found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE Node GPC.4892N Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Activated Reserved Node GPC.4892N Services
- Notify Company to request Node activation, deactivation or changes in use to production status

611112 ReliaCloud EDGE Reserved Node GPC.48153N

Definitions

AOS: Nutanix Acropolis Operating System is a Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Reserved Node GPC.48153N (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Intel processor(s), 48 cores total
- 2048 GB RAM
- Disk configuration consisting of 153.6 TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity, including but not limited to the Cluster s Node failure resiliency design, storage configurations settings, such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated, the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE Activated Reserved Node Rate (separate Item ID), until Client submits a service request for a Reserved Node to be:

  A) Removed from the Cluster, at which point the Reserved Node will remain available and billed (commencing the following month) at its Reserved Node rates;

  or

  B) Elevated to production status, at which point the Reserved Node will become part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node GPC.48153N rate (commencing the following month).

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client s request to visibility within Prism Central, is eight (8) hours. This SLO is subject to the service availability found in the SLA within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE Node GPC.48153N Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Activated Reserved Node GPC.48153N Services
- Notify Company to request Node activation, deactivation or changes in use to production status

611113 ReliaCloud EDGE Activated Reserved Node GPC.4892N.A

Company's Responsibilities and Included Features

ReliaCloud EDGE Activated Reserved Node GPC.4892N.A (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. An Activated Node is a ReliaCloud EDGE Reserved Node GPC.4892N that has been joined to an existing Cluster at Client s request and is available for Client s use.

A ReliaCloud EDGE Activated Reserved Node is identical to ReliaCloud EDGE Node GPC.4892N.A, except for the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company s responsibilities, included features, Client s responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed in whole month increments for each month that it is activated until Client submits a service request for the Activated Node to be:

A) Removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates (commencing the following month);

or

B) Elevated to production status, at which point the Activated Node will become a part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node GPC.4892N.A rate (commencing the following month).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud EDGE Node GPC.4892N.A Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Reserved Node GPC.4892N Services

611114 ReliaCloud EDGE Activated Reserved Node GPC.48153N.A

Company's Responsibilities and Included Features

ReliaCloud EDGE Activated Reserved Node GPC.48153N.A (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. An Activated Node is a ReliaCloud EDGE Reserved Node GPC.48153N that has been joined to an existing Cluster at Client s request and is available for Client s use.

A ReliaCloud EDGE Activated Reserved Node is identical to ReliaCloud EDGE Node GPC.48153N.A, except the per Node billing rate, as provided above and as otherwise provided within this ItemID. All other Company s responsibilities, included features, Client s responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed in whole month increments for each month that it is activated until Client submits a service request for the Activated Node to be:

A) Removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates (commencing the following month);

or

B) Elevated to production status, at which point the Activated Node will become a part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node GPC.48153N.A rate (commencing the following month).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud EDGE Node GPC.48153N.A Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Reserved Node GPC.48153N Services

611115 ReliaCloud EDGE Node GPC.4892N.E

Definitions

AOS: Nutanix Acropolis Operating System is a Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

VMware ESXi: VMware's hypervisor platform

Company's Responsibilities and Included Features

ReliaCloud EDGE GPC.4892N.E (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and VMware ESXi. Nodes must minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Intel processor(s), 48 cores total
- 1024 GB RAM
- Disk configuration consisting of 92.16 TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity, including but not limited to the Cluster s Node failure resiliency design, storage configuration settings, such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI (Nutanix Cloud Infrastructure) Ultimate
- Nutanix NCM (Nutanix Cloud Manager) Pro
- VMware ESXi is not included within this scope, but it is available from Company under a separate ItemID.

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive

control of Company.
- Provide continuous power to the Node via A and B side power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - Configuration and management of Challenge-Handshake Authentication (CHAP), if Company determines it as a requirement
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding (EC-X) is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates

- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company's discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

VMware System Administration:

Company will support administration of the following base features of VMware ESXi:

- Perform preventative maintenance
- Perform emergency maintenance
- Provide performance tuning
- Perform server health checks
- Perform file system maintenance
- Provision Virtual Machines (VM)
- Manage basic vSwitch network
- Manage advanced network switching (i.e. VMware vDS or other vendor supported 3rd party switch)
- Manage basic vStorage network
- Manage VMware server through vCenter
- Manage vCenter application
- Administer built-in VMware dependency components
- Provide utilization reporting

LAN management of the virtual switch is specifically excluded from this scope of Services.

VMware ESXi Triage and Troubleshooting:

- Triage of VMware ESXi incidents
- Troubleshoot and work to resolve VMware ESXi system incidents
- Document VMware ESXi system issues and errors

VMware ESXi Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the ESXi software (including major upgrades) will be conducted at Company's discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, includes:

- Ability to login into vCenter and general visibility into the Cluster metrics and configuration settings such as:

        - Cluster and VM performance and analysis
        - Cluster and health and availability
        - Cluster capacity and trend info
        - Alerts and notifications
    - Creation of customized dashboards
    - Self-service management of virtual infrastructure
        - Create, delete and modify VMs
        - Execute snapshots and restorations
        - Add VMs to catalog
        - Import, add, create and delete images to catalog
        - Create and modify data protection and recovery policies

Upon Client s request, Company will provide account(s) with administrator level and/or viewer privileges.

Company s SLA obligations will not apply to incidents caused by Client s co-administration activities. Company s remediation of Client s caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priorities 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priorities 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client, as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party ESXi enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client s business continuity plan(s) and disaster recovery plan(s) are Client s responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AOS is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.

- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

- Client agrees, acknowledges, and understands that the actual manufacture of the VMware ESXi is by VMware, Inc. and its provision and performance may be subject to change as determined by VMware, Inc.

- Client agrees that VMware ESXi offerings provided herein are subject to the VMware Services End User License Agreement available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf and privacy policy located at https://www.vmware.com/help/privacy.html, which are hereby incorporated into this Statement of Work.

611116 ReliaCloud EDGE Node GPC.48153N.E

Definitions

AOS: Nutanix Acropolis Operating System is a Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

VMware ESXi: VMware's hypervisor platform

Company's Responsibilities and Included Features

ReliaCloud EDGE GPC.48153N.E (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and VMware ESXi. Nodes must minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Intel processor(s), 48 cores total
- 2048 GB RAM
- Disk configuration consisting of 153.6 TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity, including but not limited to the Cluster s Node failure resiliency design, storage configuration settings, such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI (Nutanix Cloud Infrastructure) Ultimate
- Nutanix NCM (Nutanix Cloud Manager) Pro
- VMware ESXi is not included within this scope, but it is available from Company under a separate ItemID.

Node hosting specifications:

- Provide a secure four-sided locking cabinet to host the EDGE Node. Cabinets are multi-tenant and under the exclusive control of Company.
- Provide continuous power to the Node via A and B side power feeds

- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain physical security of the cabinet
- Provide all EDGE Node physical moves, adds and changes
- Provide two (2) network LAN connections that support up to 25 Gbps port speeds

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - Configuration and management of Challenge-Handshake Authentication (CHAP), if Company determines it as a requirement
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding (EC-X) is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client s notification of Updates
- Application of Updates during Company s defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company's

discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

VMware System Administration:

Company will support administration of the following base features of VMware ESXi:

- Perform preventative maintenance
- Perform emergency maintenance
- Provide performance tuning
- Perform server health checks
- Perform file system maintenance
- Provision Virtual Machines (VM)
- Manage basic vSwitch network
- Manage advanced network switching (i.e. VMware vDS or other vendor supported 3rd party switch)
- Manage basic vStorage network
- Manage VMware server through vCenter
- Manage vCenter application
- Administer built-in VMware dependency components
- Provide utilization reporting

LAN management of the virtual switch is specifically excluded from this scope of Services.

VMware ESXi Triage and Troubleshooting:

- Triage of VMware ESXi incidents
- Troubleshoot and work to resolve VMware ESXi system incidents
- Document VMware ESXi system issues and errors

VMware ESXi Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client s notification of Updates
- Application of Updates during Company s defined maintenance windows
- Periodic application of the Updates to the ESXi software (including major upgrades) will be conducted at Company's discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, includes:

- Ability to login into vCenter and general visibility into the Cluster metrics and configuration settings such as:
    - Cluster and VM performance and analysis
    - Cluster and health and availability

        - Cluster capacity and trend info
        - Alerts and notifications
    - Creation of customized dashboards
    - Self-service management of virtual infrastructure
        - Create, delete and modify VMs
        - Execute snapshots and restorations
        - Add VMs to catalog
        - Import, add, create and delete images to catalog
        - Create and modify data protection and recovery policies

Upon Client s request Company will provide account(s) with administrator level and/or viewer privileges.

Company s SLA obligations will not apply to incidents caused by Client s co-administration activities. Company s remediation of Client s caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client s Expert User*, available during the following hours:

- 24 x 7 technical support for priorities 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priorities 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party ESXi enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client s business continuity plan(s) and disaster recovery plan(s) are Client s responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AOS is by Nutanix, Inc., and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.

- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

- Client agrees, acknowledges, and understands that the actual manufacture of the VMware ESXi is by VMware, Inc. and its provision and performance may be subject to change as determined by VMware, Inc.

- Client agrees that VMware ESXi offerings provided herein are subject to the VMware Services End User License Agreement available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf and privacy policy located at https://www.vmware.com/help/privacy.html, which are hereby incorporated into this Statement of Work.

611117 ReliaCloud EDGE Activated Reserved Node GPC.4892N.E

Company's Responsibilities and Included Features

ReliaCloud EDGE Activated Reserved Node GPC.4892N.E (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and VMWare ESXi. An Activated Node is a ReliaCloud EDGE Reserved Node GPC.4892N that has been joined to an existing Cluster at Client s request and is available for Client s use.

A ReliaCloud EDGE Activated Reserved Node is identical to ReliaCloud EDGE Node GPC.4892N.E, except for the per Node billing rate, as provided above and as otherwise provided within this ItemID. All other Company s responsibilities, included features, Client s responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed in whole month increments for each month that it is activated until Client submits a service request for the Activated Node to be:

A) Removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates (commencing the following month);

or

B) Elevated to production status, at which point the Activated Node will become a part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node GPC.4892N.E rate (commencing the following month).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud EDGE Node GPC.4892N.E Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Reserved Node GPC.4892N Services

611118 ReliaCloud EDGE Activated Reserved Node GPC.48153N.E

Company's Responsibilities and Included Features

ReliaCloud EDGE Activated Reserved Node GPC.48153N.E (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and VMWare ESXi. An Activated Node is a ReliaCloud EDGE Reserved Node GPC.48153N that has been joined to an existing Cluster at Client s request and is available for Client s use.

A ReliaCloud EDGE Activated Reserved Node is identical to ReliaCloud EDGE Node GPC.48153N.E, except for the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company s responsibilities, included features, Client s responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed in whole month increments for each month that it is activated until Client submits a service request for the Activated Node to be:

A) Removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates

(commencing the following month);

or

B) Elevated to production status, at which point the Activated Node will become a part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node GPC.48153N.E rate (commencing the following month).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud EDGE Node GPC.48153N.E Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Reserved Node GPC.48153N Services

611130 ReliaCloud Gen 2 Private Cloud Bundle

Company's Responsibilities and Included Features

Provide Client with ReliaCloud private cloud compute and storage utilizing the currently deployed hardware on the Company's ReliaCloud generation 2 (RC2) platform up to the capacity provisioned for Client by Company as of July 1, 2024.

This service is provided at a flat fee per Company location out of which the service is provided.

Company will not be liable for any SLA penalties related to the delivery of the RC2 platform.

No additional workloads may be added to the ReliaCloud Gen 2 Private Cloud Bundle, nor may any workloads/VMs be expanded.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of any service requirements, changes or modifications
- Operating system and application licensing and supporting maintenance
- Ownership and management of Client applications
- Subscription to Company enterprise firewall services is required
- Subscription to Company provided VMware host server management is required
- Subscription to Company provided VMware software licensing is required
- VPN or WAN connectivity to server through the ReliaCloud network

611330 ReliaCloud EDGE On-Prem Node GPC.4892.2048N.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Node GPC.4892.2048N.A (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE Nodes minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Intel Processor(s), 48 cores total
- 2048 GB RAM
- Disk configuration of 92.16 TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI (Nutanix Cloud Infrastructure) Ultimate
- Nutanix NCM (Nutanix Cloud Manager) Pro

The EDGE Node includes the following Nutanix software that can be self-enrolled and disenrolled by Customer. Usage of this software may incur additional charges as defined by the Agreement:

- Nutanix Unified Storage Pro Per TiB
- Nutanix Unified Storage Starter Per TiB

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression

        - Deduplication
        - Erasure coding (EC-X) *
    - Nutanix Volumes Management
        - Creation of iSCSI volume group(s)
        - Management of volume groups
        - Management of client iSCSI initiators
        - Management of iSCSI data services
        - Configure Bare Metal Nodes for IP addressing
        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
    - Infrastructure Resilience
        - Data path redundancy
        - Tunable redundancy factor
    - Security
        - Client authentication
        - Cluster lockdown
        - Data-at-rest encryption (software-based and self-encrypting drives)
    - Management and Analytics
        - Prism Central and Prism Elements
        - PulseCluster health

* Erasure coding (EC-X) is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node maintenance management is limited to:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client s notification of Updates
- Application of Updates during Company s defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features are available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
    - Cluster and VM performance and analysis
    - Cluster, health and availability
    - Cluster capacity and trend info

        - Alerts and notifications
    - Creation of customized dashboards
    - Self-service management of virtual infrastructure
        - Create, delete and modify VMs
        - Execute snapshots and restorations
        - Add VMs to catalog
        - Import, add, create and delete images to catalog
        - Create and modify data protection and recovery policies

Upon Client s written request, Company will provide account(s) with administrator level and or viewer privileges.

Company s SLA obligations will not apply to incidents caused by Client s co-administration activities. Company s remediation of Client s caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client s Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

End of Service Equipment Return

- Company will provide to Client packing materials, prepaid shipping label, and return instructions.
- Professional Services are available for unracking, packing and decommission of equipment under a separate statement of work.
- Company will continue to charge for the supplied On-Prem equipment at the contracted rates until Company takes physical receipt of the assets.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hosting specifications:

Client must complete an environment readiness assessment for Company provided equipment:

- Provide location information of where the EDGE Node will be housed:
    - Address, City, State, Zip
    - On premise contact information Name, email address, phone number
- House the EDGE Node within a power and climate-controlled location that is appropriate for computer and IT storage equipment.

EDGE Node specifications per Node, Client s failure to meet these specifications will excuse Company from availability SLAs:

Min Cluster Size	3 Nodes

Power Ranges Per Node	700W Typical 1600W maximum
Power Delivery	Continuous feeds 2x 208V 20 Amp
Operating Requirements	Input Voltage: 100-240V AC auto-range, Input Frequency: 50-60Hz
Power Diversity	A & B UPS + Backup Power (generator)
Operating Environment	Op Temp Range: 50 to 95 F (10 to 35 C) Op Humidity Range (non-condensing): 68 to 194 F (20 to 90 C)
Rough Dimensions Per Node	Height: 1.69" Width: 17.11" Depth: 30.43" Rack Units: 2U
Network Connections Per Node	2 x 25 Gbps SFP 1 x 1 GbE (TX)

- The Service Level Objective (SLO) for repair or replacement is next business day or better.
- Provide a secure cabinet or other approved Company enclosure to house EDGE Node
- Maintain environmental standards for HVAC consistent with primary hosting facility.
- Maintain physical security of the cabinet.
- Connect the Network Switch48 to Client s network core if applicable.
- Open any necessary firewall or network ports and conduits to allow a connection between the EDGE Node and the Company s network operation center.
- Assist with any physical interaction for EDGE Node repair or replacement as needed, and provide escorted access to the EDGE Node for Company and/or Company s authorized service vendor.
- Coordinate all Client responsibilities outlined herein, including all necessary communication to Client personnel.
- Provide or purchase all necessary equipment, cabling, circuits, and other materials required for the services, unless OneNeck explicitly provides that such materials are included as part of the services.
- Ensure compliance with any national or local safety standard or similar requirement affecting the installation of the EDGE Node.
- Provide Company with access, passwords, access codes or security devices as necessary to perform the services.

End of Service Equipment Return

Upon termination of this service, Client must return the equipment in good working condition to Company. The procedure to initiate equipment returns is to create a ticket with the Company Service Desk. This can be conducted via phone, email, or web portal. Additional activities include:

- Unrack, remove cables, and pack Company s provided equipment into Company s provided return shipping materials.
- Coordinate transfer of equipment to Company s specified courier.
- Ship all devices to OneNeck within five (5) business days after receipt of Company s provided packing materials.

- Equipment not returned within five (5) business days after receipt of Company s provided packing materials will be billed at existing company s rates, until received by Company s specified courier.

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment
- This platform includes software features that are Customer discoverable and allow for self-enrollment. These services are metered usage and will bill monthly based upon their usage. The following ItemIDs must be subscribed to, but don't require their use unless desired by Customer:
  - 611388 Nutanix Unified Storage Pro Per TiB
  - 61138 Nutanix Unified Storage Starter Per TiB
- Subscribe to Company Remote Management Infrastructure (1-24 devices) service, ItemID 500159

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are solely Client s responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to, and governed by, the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full

611331 ReliaCloud EDGE On-Prem Reserved Activated Node GPC.4892.2048N.A

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Reserved Activated Node GPC.4892.2048N.A (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. An Activated Node is a ReliaCloud EDGE On-Prem Reserved Node GPC.4892.2048N.A that has been joined to an existing Cluster at Client request and is available for Client s use.

A ReliaCloud EDGE On-Prem Reserved Activated Node is identical to ReliaCloud EDGE On-Prem Node GPC.4892.2048N.A, except the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company responsibilities, included features, Client responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed monthly in whole day increments for each day that it is activated until Client submits a service request for the Activated Node to be:

A) Removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates.

or

B) Elevated to production status, at which point the Activated Node will become a part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE On-Prem Node GPC.4892.2048N.A rate.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud EDGE On-Prem Node GPC.4892.2048N.A Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE On-Prem Reserved Node GPC.4892.2048N.A Services

611332 ReliaCloud EDGE On-Prem Reserved Node GPC.4892.2048N

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Reserved Node GPC.4892.2048N (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Intel Processor(s), 48 cores total
- 2048 GB RAM
- Disk configuration of 92.16TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business

and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE On-Prem Activated Reserved Node Rate, until Client submits a service request for a Reserved Node to be removed from the Cluster, at which point the Reserved Node will remain available and billied at its Reserved Note rates.

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE On-Prem Node GPC.4892.2048N Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud On-Prem EDGE Reserved Activated Node GPC.4892.2048N Services
- Notify Company to request Node activation, deactivation or changes in use to production status

611499 ReliaCloud EDGE On-Prem Node GPC.3292N.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Node GPC.3292N.A (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE Nodes minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Intel Processor(s), 32 cores total
- 1024 GB RAM
- Disk configuration of 92.16 TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI (Nutanix Cloud Infrastructure) Ultimate
- Nutanix NCM (Nutanix Cloud Manager) Pro

The EDGE Node includes the following Nutanix software that can be self-enrolled and disenrolled by Customer. Usage of this software may incur additional charges as defined by the Agreement:

- Nutanix Unified Storage Pro Per TiB
- Nutanix Unified Storage Starter Per TiB

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
  - Cluster sizing including heterogeneous Clusters
  - Data tiering
  - Inline compression
  - Inline performance deduplication
  - Online Cluster growth
  - Compression
  - Deduplication
  - Erasure coding (EC-X) *
- Nutanix Volumes Management
  - Creation of iSCSI volume group(s)
  - Management of volume groups
  - Management of client iSCSI initiators

Management of iSCSI data services
        - Configure Bare Metal Nodes for IP addressing
        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - PulseCluster health

* Erasure coding (EC-X) is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node maintenance management is limited to:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client s notification of Updates
- Application of Updates during Company s defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features are available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
    - Cluster and VM performance and analysis
    - Cluster, health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog

- Import, add, create and delete images to catalog
- Create and modify data protection and recovery policies

Upon Client s written request, Company will provide account(s) with administrator level and or viewer privileges.

Company s SLA obligations will not apply to incidents caused by Client s co-administration activities. Company s remediation of Client s caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client s Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

End of Service Equipment Return

- Company will provide to Client packing materials, prepaid shipping label, and return instructions.
- Professional Services are available for unracking, packing and decommission of equipment under a separate statement of work.
- Company will continue to charge for the supplied On-Prem equipment at the contracted rates until Company takes physical receipt of the assets.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hosting specifications:

Client must complete an environment readiness assessment for Company provided equipment:

- Provide location information of where the EDGE Node will be housed:
  - Address, City, State, Zip
  - On premise contact information Name, email address, phone number
- House the EDGE Node within a power and climate-controlled location that is appropriate for computer and IT storage equipment.

EDGE Node specifications per Node, Client s failure to meet these specifications will excuse Company from availability SLAs:

Min Cluster Size	3 Nodes
Power Ranges Per Node	700W Typical 1600W maximum
Power Delivery	Continuous feeds 2x 208V 20 Amp
Operating Requirements	Input Voltage: 100-240V AC auto-range, Input Frequency: 50-60Hz
Power Diversity	A & B UPS + Backup Power (generator)

Operating Environment	Op Temp Range: 50 to 95 F (10 to 35 C) Op Humidity Range (non-condensing): 68 to 194 F (20 to 90 C)
Rough Dimensions Per Node	Height: 1.69" Width: 17.11" Depth: 30.43" Rack Units: 2U
Network Connections Per Node	2 x 25 Gbps SFP 1 x 1 GbE (TX)

- The Service Level Objective (SLO) for repair or replacement is next business day or better.
- Provide a secure cabinet or other approved Company enclosure to house EDGE Node
- Maintain environmental standards for HVAC consistent with primary hosting facility.
- Maintain physical security of the cabinet.
- Connect the Network Switch48 to Client s network core if applicable.
- Open any necessary firewall or network ports and conduits to allow a connection between the EDGE Node and the Company s network operation center.
- Assist with any physical interaction for EDGE Node repair or replacement as needed, and provide escorted access to the EDGE Node for Company and/or Company s authorized service vendor.
- Coordinate all Client responsibilities outlined herein, including all necessary communication to Client personnel.
- Provide or purchase all necessary equipment, cabling, circuits, and other materials required for the services, unless OneNeck explicitly provides that such materials are included as part of the services.
- Ensure compliance with any national or local safety standard or similar requirement affecting the installation of the EDGE Node.
- Provide Company with access, passwords, access codes or security devices as necessary to perform the services.

End of Service Equipment Return

Upon termination of this service, Client must return the equipment in good working condition to Company. The procedure to initiate equipment returns is to create a ticket with the Company Service Desk. This can be conducted via phone, email, or web portal. Additional activities include:

- Unrack, remove cables, and pack Company s provided equipment into Company s provided return shipping materials.
- Coordinate transfer of equipment to Company s specified courier.
- Ship all devices to OneNeck within five (5) business days after receipt of Company s provided packing materials.
- Equipment not returned within five (5) business days after receipt of Company s provided packing materials will be billed at existing company s rates, until received by Company s specified courier.

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment
- This platform includes software features that are Customer discoverable and allow for self-enrollment. These services are metered usage and will bill monthly based upon their usage. The following ItemIDs must be subscribed to, but don't require their use unless desired by Customer:
    - 611388 Nutanix Unified Storage Pro Per TiB
    - 611389 Nutanix Unified Storage Starter Per TiB
- Subscribe to Company Remote Management Infrastructure (1-24 devices) service, ItemID 500159

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are solely Client s responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to, and governed by, the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full

611500 ReliaCloud EDGE On-Prem Reserved Activated Node GPC.3292N.A

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Reserved Activated Node GPC.3292N.A (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. An Activated Node is a ReliaCloud EDGE On-Prem Reserved Node GPC.3292N.A that has been joined to an existing Cluster at Client request and is available for Client s use.

A ReliaCloud EDGE On-Prem Reserved Activated Node is identical to ReliaCloud EDGE On-Prem Node GPC.3292N.A, except the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company responsibilities, included features, Client responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed monthly in whole day increments for each day that it is activated until Client submits a service request for the Activated Node to be:

A) Removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates.

or

B) Elevated to production status, at which point the Activated Node will become a part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE On-Prem Node GPC.3292N.A rate.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud EDGE On-Prem Node GPC.3292N.A Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE On-Prem Reserved Node GPC.3292N.A Services

611501 ReliaCloud EDGE On-Prem Reserved Node GPC.3292N

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Reserved Node GPC.3292N (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Intel Processor(s), 32 cores total
- 1024 GB RAM
- Disk configuration of 92.16TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE On-Prem Activated Reserved Node Rate, until Client submits a service request for a Reserved Node to be removed from the Cluster, at which point the Reserved Node will remain available and billied at its Reserved Note rates.

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE On-Prem Node GPC.3292N Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud On-Prem EDGE Reserved Activated Node GPC.3292N Services
- Notify Company to request Node activation, deactivation or changes in use to production status

611502 ReliaCloud EDGE On-Prem Node GPC.4892N.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Node GPC.4892N.A (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE Nodes minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Intel Processor(s), 48 cores total
- 1024 GB RAM
- Disk configuration of 92.16 TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI (Nutanix Cloud Infrastructure) Ultimate
- Nutanix NCM (Nutanix Cloud Manager) Pro

The EDGE Node includes the following Nutanix software that can be self-enrolled and disenrolled by Customer. Usage of this software may incur additional charges as defined by the Agreement:

- Nutanix Unified Storage Pro Per TiB
- Nutanix Unified Storage Starter Per TiB

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
    - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor

- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - PulseCluster health

* Erasure coding (EC-X) is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node maintenance management is limited to:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode

- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client s notification of Updates
- Application of Updates during Company s defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features are available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
    - Cluster and VM performance and analysis
    - Cluster, health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection and recovery policies

Upon Client s written request, Company will provide account(s) with administrator level and or viewer privileges.

Company s SLA obligations will not apply to incidents caused by Client s co-administration activities. Company s remediation of Client s caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client s Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

End of Service Equipment Return

- Company will provide to Client packing materials, prepaid shipping label, and return instructions.
- Professional Services are available for unracking, packing and decommission of equipment under a separate statement of work.
- Company will continue to charge for the supplied On-Prem equipment at the contracted rates until Company takes physical receipt of the assets.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hosting specifications:

Client must complete an environment readiness assessment for Company provided equipment:

- Provide location information of where the EDGE Node will be housed:
  - Address, City, State, Zip
  - On premise contact information Name, email address, phone number
- House the EDGE Node within a power and climate-controlled location that is appropriate for computer and IT storage equipment.

EDGE Node specifications per Node, Client s failure to meet these specifications will excuse Company from availability SLAs:

Min Cluster Size	3 Nodes
Power Ranges Per Node	700W Typical 1600W maximum
Power Delivery	Continuous feeds 2x 208V 20 Amp
Operating Requirements	Input Voltage: 100-240V AC auto-range, Input Frequency: 50-60Hz
Power Diversity	A & B UPS + Backup Power (generator)
Operating Environment	Op Temp Range: 50 to 95 F (10 to 35 C) Op Humidity Range (non-condensing): 68 to 194 F (20 to 90 C)
Rough Dimensions Per Node	Height: 1.69" Width: 17.11"

	Depth: 30.43" Rack Units: 2U
Network Connections Per Node	2 x 25 Gbps SFP 1 x 1 GbE (TX)

- The Service Level Objective (SLO) for repair or replacement is next business day or better.
- Provide a secure cabinet or other approved Company enclosure to house EDGE Node
- Maintain environmental standards for HVAC consistent with primary hosting facility.
- Maintain physical security of the cabinet.
- Connect the Network Switch48 to Client s network core if applicable.
- Open any necessary firewall or network ports and conduits to allow a connection between the EDGE Node and the Company s network operation center.
- Assist with any physical interaction for EDGE Node repair or replacement as needed, and provide escorted access to the EDGE Node for Company and/or Company s authorized service vendor.
- Coordinate all Client responsibilities outlined herein, including all necessary communication to Client personnel.
- Provide or purchase all necessary equipment, cabling, circuits, and other materials required for the services, unless OneNeck explicitly provides that such materials are included as part of the services.
- Ensure compliance with any national or local safety standard or similar requirement affecting the installation of the EDGE Node.
- Provide Company with access, passwords, access codes or security devices as necessary to perform the services.

End of Service Equipment Return

Upon termination of this service, Client must return the equipment in good working condition to Company. The procedure to initiate equipment returns is to create a ticket with the Company Service Desk. This can be conducted via phone, email, or web portal. Additional activities include:

- Unrack, remove cables, and pack Company s provided equipment into Company s provided return shipping materials.
- Coordinate transfer of equipment to Company s specified courier.
- Ship all devices to OneNeck within five (5) business days after receipt of Company s provided packing materials.
- Equipment not returned within five (5) business days after receipt of Company s provided packing materials will be billed at existing company s rates, until received by Company s specified courier.

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

- This platform includes software features that are Customer discoverable and allow for self-enrollment. These services are metered usage and will bill monthly based upon their usage. The following ItemIDs must be subscribed to, but don't require their use unless desired by Customer:
  - 611388 Nutanix Unified Storage Pro Per TiB
  - 611389 Nutanix Unified Storage Starter Per TiB
- Subscribe to Company Remote Management Infrastructure (1-24 devices) service, ItemID 500159

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are solely Client s responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to, and governed by, the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full

611503 ReliaCloud EDGE On-Prem Reserved Activated Node GPC.4892N.A

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Reserved Activated Node GPC.4892N.A (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. An Activated Node is a ReliaCloud EDGE On-Prem Reserved Node GPC.4892N.A that has been joined to an existing Cluster at Client request and is available for Client s use.

A ReliaCloud EDGE On-Prem Reserved Activated Node is identical to ReliaCloud EDGE On-Prem Node GPC.4892N.A, except the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company responsibilities, included features, Client responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed monthly in whole day increments for each day that it is activated until Client submits a service request for the Activated Node to be:

A) Removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates.

or

B) Elevated to production status, at which point the Activated Node will become a part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE On-Prem Node GPC.4892N.A rate.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud EDGE On-Prem Node GPC.4892N.A Services and have a Cluster of at least three (3) Nodes

611504 ReliaCloud EDGE On-Prem Reserved Node GPC.4892N

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Reserved Node GPC.4892N (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Intel Processor(s), 48 cores total
- 1024 GB RAM
- Disk configuration of 92.16TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE On-Prem Activated Reserved Node Rate, until Client submits a service request for a Reserved Node to be removed from the Cluster, at which point the Reserved Node will remain available and billed at its Reserved Note rates.

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE On-Prem Node GPC.4892N Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud On-Prem EDGE Reserved Activated Node GPC.4892N Services
- Notify Company to request Node activation, deactivation or changes in use to production status

611505 ReliaCloud EDGE On-Prem Node GPC.1630N.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Node GPC.1630N.A (EDGE Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE Nodes minimally belong to a Cluster configured with at least three (3) EDGE Nodes. EDGE Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Intel Processor(s), 16 cores total
- 512 GB RAM
- Disk configuration of 30.72 TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node software specifications:

Company will provide an EDGE Node that provides a software release that meets or exceeds the following software editions:

- Nutanix NCI (Nutanix Cloud Infrastructure) Ultimate
- Nutanix NCM (Nutanix Cloud Manager) Pro

The EDGE Node includes the following Nutanix software that can be self-enrolled and disenrolled by Customer. Usage of this software may incur additional charges as defined by the Agreement:

- Nutanix Unified Storage Pro Per TiB
- Nutanix Unified Storage Starter Per TiB

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
    - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements

- PulseCluster health

* Erasure coding (EC-X) is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node maintenance management is limited to:

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features

- VM management. VM s operating system management and application management is specifically excluded from this scope.
- VM automated resource scheduling
- VM affinity rules
- Virtual network configuration
- Host profiles
- VM high availability
- Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client s notification of Updates
- Application of Updates during Company s defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with standard industry practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features are available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
  - Cluster and VM performance and analysis
  - Cluster, health and availability
  - Cluster capacity and trend info
  - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
  - Create, delete and modify VMs
  - Execute snapshots and restorations
  - Add VMs to catalog
  - Import, add, create and delete images to catalog
  - Create and modify data protection and recovery policies

Upon Client s written request, Company will provide account(s) with administrator level and or viewer privileges.

Company s SLA obligations will not apply to incidents caused by Client s co-administration activities. Company s remediation of Client s caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client s Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents

- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

End of Service Equipment Return

- Company will provide to Client packing materials, prepaid shipping label, and return instructions.
- Professional Services are available for unracking, packing and decommission of equipment under a separate statement of work.
- Company will continue to charge for the supplied On-Prem equipment at the contracted rates until Company takes physical receipt of the assets.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hosting specifications:

Client must complete an environment readiness assessment for Company provided equipment:

- Provide location information of where the EDGE Node will be housed:
  - Address, City, State, Zip
  - On premise contact information Name, email address, phone number
- House the EDGE Node within a power and climate-controlled location that is appropriate for computer and IT storage equipment.

EDGE Node specifications per Node, Client s failure to meet these specifications will excuse Company from availability SLAs:

Min Cluster Size	3 Nodes
Power Ranges Per Node	700W Typical 1600W maximum
Power Delivery	Continuous feeds 2x 208V 20 Amp
Operating Requirements	Input Voltage: 100-240V AC auto-range, Input Frequency: 50-60Hz
Power Diversity	A & B UPS + Backup Power (generator)
Operating Environment	Op Temp Range: 50 to 95 F (10 to 35 C) Op Humidity Range (non-condensing): 68 to 194 F (20 to 90 C)
Rough Dimensions Per Node	Height: 1.69" Width: 17.11" Depth: 30.43" Rack Units: 2U
Network Connections Per Node	2 x 25 Gbps SFP 1 x 1 GbE (TX)

- The Service Level Objective (SLO) for repair or replacement is next business day or better.
- Provide a secure cabinet or other approved Company enclosure to house EDGE Node
- Maintain environmental standards for HVAC consistent with primary hosting facility.
- Maintain physical security of the cabinet.
- Connect the Network Switch48 to Client s network core if applicable.
- Open any necessary firewall or network ports and conduits to allow a connection between the EDGE Node and the Company s network operation center.
- Assist with any physical interaction for EDGE Node repair or replacement as needed, and provide escorted access to the EDGE Node for Company and/or Company s authorized service vendor.
- Coordinate all Client responsibilities outlined herein, including all necessary communication to Client personnel.
- Provide or purchase all necessary equipment, cabling, circuits, and other materials required for the services, unless OneNeck explicitly provides that such materials are included as part of the services.
- Ensure compliance with any national or local safety standard or similar requirement affecting the installation of the EDGE Node.
- Provide Company with access, passwords, access codes or security devices as necessary to perform the services.

End of Service Equipment Return

Upon termination of this service, Client must return the equipment in good working condition to Company. The procedure to initiate equipment returns is to create a ticket with the Company Service Desk. This can be conducted via phone, email, or web portal. Additional activities include:

- Unrack, remove cables, and pack Company s provided equipment into Company s provided return shipping materials.
- Coordinate transfer of equipment to Company s specified courier.
- Ship all devices to OneNeck within five (5) business days after receipt of Company s provided packing materials.
- Equipment not returned within five (5) business days after receipt of Company s provided packing materials will be billed at existing company s rates, until received by Company s specified courier.

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment
- This platform includes software features that are Customer discoverable and allow for self-enrollment. These services are metered usage and will bill monthly based upon their usage. The following ItemIDs must be subscribed to, but don't require their use unless desired by Customer:
    - 611388 Nutanix Unified Storage Pro Per TiB
    - 611389 Nutanix Unified Storage Starter Per TiB
- Subscribe to Company Remote Management Infrastructure (1-24 devices) service, ItemID 500159

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are solely Client s responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to, and governed by, the Nutanix License and Service Agreement available at https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full

611506 ReliaCloud EDGE On-Prem Reserved Activated Node GPC.1630N.A

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Reserved Node GPC.1630N (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Intel Processor(s), 16 cores total
- 512 GB RAM
- Disk configuration of 30.72TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is

determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE On-Prem Activated Reserved Node Rate, until Client submits a service request for a Reserved Node to be removed from the Cluster, at which point the Reserved Node will remain available and billed at its Reserved Note rates.

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE On-Prem Node GPC.1630N Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud On-Prem EDGE Reserved Activated Node GPC.1630N Services
- Notify Company to request Node activation, deactivation or changes in use to production status

611507 ReliaCloud EDGE On-Prem Reserved Node GPC.1630N

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Reserved Node GPC.1630N (Reserved Node) provides an allocation of compute resources to an

existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Intel Processor(s), 16 cores total
- 512 GB RAM
- Disk configuration of 30.72TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE On-Prem Activated Reserved Node Rate, until Client submits a service request for a Reserved Node to be removed from the Cluster, at which point the Reserved Node will remain available and billed at its Reserved Note rates.

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE On-Prem Node GPC.1630N Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud On-Prem EDGE Reserved Activated Node GPC.1630N Services
- Notify Company to request Node activation, deactivation or changes in use to production status

Category: Public Cloud

110011 Public Cloud (VMware) - Additional GHz

Company's Responsibilities and Included Features

- Deliver additional vCPUs in increments of 1.0 Ghz
- Deliver a maximum vCPUs per VM of 8

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Adjust per VM resource allocations

500063 Public Cloud v2 (VMware) MEM

Company's Responsibilities and Included Features

The ReliaCloud Public Cloud service delivers a compute resource solution leveraging our enterprise compute, network and storage resources which help Clients avoid a large capital outlay but still fulfill their business requirements. The Client will selectively leverage management services for applications that fall outside of their core competencies. Management of the ESX hosts is Company responsibility. Management of the operating system and application layers can be provided by Company or can be managed by the Client s staff. Company will deliver public compute resources which the Client can manage and provision with a web interface. Public Cloud is defined as shared physical hardware, hypervisor software (VMware ESX) and shared storage. Data is electronically isolated and segmented from Client to Client leveraging the hypervisor software. The environment is designed in a highly available nature with sufficient infrastructure to withstand the loss of at least a single critical component.

- Provide enterprise compute resources which the client can maintain and provision via a web interface
- Delivered on shared physical hardware and hypervisor software (VMware ESX)
- Provide an environment which is electronically isolated and segmented from client to client leveraging the hypervisor software
- Delivery RAM resource pool in 1 GB increments. Maximum per Virtual Machine (VM) is 128 GB
- Deliver a maximum vCPU speed 3.0 Ghz
- Deliver a maximum vCPUs per VM of 10
- Deliver an aggregate of .234 GHz per 1 GB of RAM delivered to the processor pool. With a minimum pool size of 3 GHz CPU.
- Configure access to vCloud Director management interface
- Windows Server operating system licensing included
- 24/7 expert engineering support on compute infrastructure
- All infrastructure management and capacity planning activities
- Maintain public image catalog
- Infrastructure maintenance and support, including vendor and licensing management
- Provide access to management platform to administer the cloud infrastructure (vCloud Director)
- Provide VMware ESX licensing
- Provide (if applicable) Windows operating system licensing
- Monitor availability of the host machines
- Notify Client of any detected host level issues.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of any service requirements, changes or modifications
- Non-Windows operating systems and application licensing and supporting maintenance other than the software associated with the hypervisor
- Ownership of application and operating system support and management
- Resource pool management

- Maintenance of VMs, vAPPs and the vAPP templates
- Manipulation of VM resources to meet performance expectations
- Adjust per VM resource allocations

601724 ReliaCloud ELASTIC Protected VM-GPXS

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System

Availability Zone: A location to which one can replicate VM data for protection, represented by a Prism Central instance to which a Nutanix Cluster is registered

Cluster: A logical grouping of Nodes and software to form an IT services entity

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Primary VM: A VM that is the primary source of where a production workload is run. It is also the source VM from which Snapshots are taken

Protected VM: The Primary VM that is designated to be protected by the ReliaCloud ELASTIC Protected VM service. The Primary VM resides on the Client s Nutanix AOS-based AHV Cluster, which is a separate Availability Zone and/or location from the ReliaCloud ELASTIC service environment.

Protection Policy: A combination of scheduled and configurable parameters that define how often a Snapshot of a VM is taken, how long the Snapshot is retained for, and where the Snapshot is stored

Replication Network: A network connection between the primary and recovery sites with sufficient bandwidth to accommodate the RPO requirements

RPO: Recovery Point Objective: The targeted maximum amount of data that will be unavailable in the Disaster Recovery (DR) system in terms of time, backwards from the point of disaster.

Snapshot: A point in time copy of a VM which is facilitated by the hypervisor

VM: Virtual machine

Company's Responsibilities and Included Features

ReliaCloud ELASTIC Protected VM-GPXS (VM-GPXS) service is comprised of compute resources which includes storage space for replicated Snapshots and the ability to power on, run, and operate the replicated VM at Client s discretion. This service is applied to a single Primary VM that meets the compute sizing specifications of the VM-GXPS listed below.

VM-GPXS specifications

The VM-GPXS is designed as a general-purpose performance VM. Company will provide compute resources for a Primary VM with the following specifications:

- 1 vCPU
- 2 GB RAM
- 40 GB O/S Drive

Protection of the Primary VM includes:

- Creation of protection policy(ies) based on Client-provided objectives (collectively Protection Policy)
- Application of the Protection Policy to the Primary VM
- Execution of the Protection Policy

- Replication of Snapshots of the Protected VM to Company s ReliaCloud ELASTIC Cluster at an interval determined by Client and Company and then applied by Company

Powered-On / Powered-Off Status

Protected VMs are replicated to the ReliaCloud ELASTIC Cluster in a powered-off state and remain powered off until powered on. In order to utilize the replicated VM, Client must request Company power the VM on. Client may request the replicated VM to be powered on for testing, fail-over, long-term production or other purposes. During a fail-over event, replication services will not be available until another fail-over or fail-back target is agreed to by Company and Client and setup by Company to restart replication services.

Service Metering

- This Service is a metered service
- The Service is billed against each Protected VM that matches the specifications of the VM-GXPS
- The existence of the Protected VM s data within the ReliaCloud ELASTIC cluster will count towards the number of VMs being billed that month. The existence of the Protected VM s data will count towards service billing regardless of the VM s powered state.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Approval of Company-provided Protection Policy
- Notify Company of any requirements or modifications requested to the Services
- Application licensing and supporting maintenance including the hypervisor (if not AHV),VM operating system licensing and support maintenance.
- All file system or file level backups
- Management of network devices
- Migrating VMs on or off the platform

Third-Party Utilities and Applications

- Management of third-party enhancement tools, utilities or applications

Minimum Requirements

For each Protected VM:

- Subscription to Company Managed Services for VM DR administration
- Size the Protected VM to meet the specifications of the VM-GPXS as defined above

For each recovery site:

- Provide a Replication Network
- Provide firewall

Security of all Client environments (unless specifically subscribed to Company provided security services)

Business Continuity / Disaster Recovery Plan

A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation following a disaster or interruption in business.

DR configuration activities including but not limited to the following:

- DR recovery retention window
- Server startup sequencing and startup delay
- Network mapping
- Reconfiguration of server IP address (re-IP) plan (if applicable)

Applications and Client-Side DR Configuration and Testing:

- Maintain DR test and failover procedures for all databases and applications existing on the servers included in the DR plan
- Database and application management and reconfiguration during DR testing or failover\
- Configuration of end-user devices and/or Client infrastructure required to allow end users to access the environment
- Conducting functional and data validation testing during server failover testing

601725 ReliaCloud ELASTIC Protected VM-GPS

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System

Availability Zone: A location to which one can replicate VM data for protection, represented by a Prism Central instance to which a Nutanix Cluster is registered

Cluster: A logical grouping of Nodes and software to form an IT services entity

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Primary VM: A VM that is the primary source of where a production workload is run. It is also the source VM from which Snapshots are taken

Protected VM: The Primary VM that is designated to be protected by the ReliaCloud ELASTIC Protected VM service. The Primary VM resides on the Client s Nutanix AOS-based AHV Cluster, which is a separate Availability Zone and/or location from the ReliaCloud ELASTIC service environment.

Protection Policy: A combination of scheduled and configurable parameters that define how often a Snapshot of a VM is taken, how long the Snapshot is retained for, and where the Snapshot is stored

Replication Network: A network connection between the primary and recovery sites with sufficient bandwidth to accommodate the RPO requirements

RPO: Recovery Point Objective: The targeted maximum amount of data that will be unavailable in the Disaster Recovery (DR) system in terms of time, backwards from the point of disaster.

Snapshot: A point in time copy of a VM which is facilitated by the hypervisor

VM: Virtual machine

Company's Responsibilities and Included Features

ReliaCloud ELASTIC Protected VM-GPS (VM-GPS) service is comprised of compute resources which includes storage space for

replicated Snapshots and the ability to power on, run, and operate the replicated VM at Client s discretion. This service is applied to a single Primary VM that meets the compute sizing specifications of the VM-GPS listed below.

VM-GPS specifications

The VM-GPS is designed as a general-purpose performance VM. Company will provide compute resources for a Primary VM with the following specifications:

- 1 vCPU
- 4 GB RAM
- 80 GB O/S Drive
- 50 GB Data Drive

Protection of the Primary VM includes:

- Creation of protection policy(ies) based on Client-provided objectives (collectively Protection Policy)
- Application of the Protection Policy to the Primary VM
- Execution of the Protection Policy
- Replication of Snapshots of the Protected VM to Company s ReliaCloud ELASTIC Cluster at an interval determined by Client and Company and then applied by Company

Powered-On / Powered-Off Status

Protected VMs are replicated to the ReliaCloud ELASTIC Cluster in a powered-off state and remain powered off until powered on. In order to utilize the replicated VM, Client must request Company power the VM on. Client may request the replicated VM to be powered on for testing, fail-over, long-term production or other purposes. During a fail-over event, replication services will not be available until another fail-over or fail-back target is agreed to by Company and Client and setup by Company to restart replication services.

Service Metering

- This Service is a metered service
- The Service is billed against each Protected VM that matches the specifications of the VM-GPS
- The existence of the Protected VM s data within the ReliaCloud ELASTIC cluster will count towards the number of VMs being billed that month. The existence of the Protected VM s data will count towards service billing regardless of the VM s powered state.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Approval of Company-provided Protection Policy
- Notify Company of any requirements or modifications requested to the Services
- Application licensing and supporting maintenance including the hypervisor (if not AHV),VM operating system licensing and support maintenance.
- All file system or file level backups
- Management of network devices

- Migrating VMs on or off the platform

Third-Party Utilities and Applications

- Management of third-party enhancement tools, utilities or applications

Minimum Requirements

For each Protected VM:

- Subscription to Company Managed Services for VM DR administration
- Size the Protected VM to meet the specifications of the VM-GPS as defined above

For each recovery site:

- Provide a Replication Network
- Provide firewall

Security of all Client environments (unless specifically subscribed to Company provided security services)

Business Continuity / Disaster Recovery Plan

A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation following a disaster or interruption in business.

DR configuration activities including but not limited to the following:

- DR recovery retention window
- Server startup sequencing and startup delay
- Network mapping
- Reconfiguration of server IP address (re-IP) plan (if applicable)

Applications and Client-Side DR Configuration and Testing:

- Maintain DR test and failover procedures for all databases and applications existing on the servers included in the DR plan
- Database and application management and reconfiguration during DR testing or failover
- Configuration of end-user devices and/or Client infrastructure required to allow end users to access the environment
- Conducting functional and data validation testing during server failover testing

601726 ReliaCloud ELASTIC Protected VM-GPM

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System

Availability Zone: A location to which one can replicate VM data for protection, represented by a Prism Central instance to which a Nutanix Cluster is registered

Cluster: A logical grouping of Nodes and software to form an IT services entity

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Primary VM: A VM that is the primary source of where a production workload is run. It is also the source VM from which Snapshots are taken

Protected VM: The Primary VM that is designated to be protected by the ReliaCloud ELASTIC Protected VM service. The

Primary VM resides on the Client s Nutanix AOS-based AHV Cluster, which is a separate Availability Zone and/or location from the ReliaCloud ELASTIC service environment.

Protection Policy: A combination of scheduled and configurable parameters that define how often a Snapshot of a VM is taken, how long the Snapshot is retained for, and where the Snapshot is stored

Replication Network: A network connection between the primary and recovery sites with sufficient bandwidth to accommodate the RPO requirements

RPO: Recovery Point Objective: The targeted maximum amount of data that will be unavailable in the Disaster Recovery (DR) system in terms of time, backwards from the point of disaster.

Snapshot: A point in time copy of a VM which is facilitated by the hypervisor

VM: Virtual machine

Company's Responsibilities and Included Features

ReliaCloud ELASTIC Protected VM-GPM (VM-GPM) service is comprised of compute resources which includes storage space for replicated Snapshots and the ability to power on, run, and operate the replicated VM at Client s discretion. This service is applied to a single Primary VM that meets the compute sizing specifications of the VM-GPM listed below.

VM-GPM specifications

The VM-GPM is designed as a general-purpose performance VM. Company will provide compute resources for a Primary VM with the following specifications:

- 2 vCPU
- 8 GB RAM
- 80 GB O/S Drive
- 250 GB Data Drive

Protection of the Primary VM includes:

- Creation of protection policy(ies) based on Client-provided objectives (collectively Protection Policy)
- Application of the Protection Policy to the Primary VM
- Execution of the Protection Policy
- Replication of Snapshots of the Protected VM to Company s ReliaCloud ELASTIC Cluster at an interval determined by Client and Company and then applied by Company

Powered-On / Powered-Off Status

Protected VMs are replicated to the ReliaCloud ELASTIC Cluster in a powered-off state and remain powered off until powered on. In order to utilize the replicated VM, Client must request Company power the VM on. Client may request the replicated VM to be powered on for testing, fail-over, long-term production or other purposes. During a fail-over event, replication services will not be available until another fail-over or fail-back target is agreed to by Company and Client and setup by Company to restart replication services.

Service Metering

- This Service is a metered service
- The Service is billed against each Protected VM that matches the specifications of the VM-GPM
- The existence of the Protected VM s data within the ReliaCloud ELASTIC cluster will count towards the number of VMs being billed that month. The existence of the Protected VM s data will count towards service billing regardless of the VM s powered state.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Approval of Company-provided Protection Policy
- Notify Company of any requirements or modifications requested to the Services
- Application licensing and supporting maintenance including the hypervisor (if not AHV),VM operating system licensing and support maintenance.
- All file system or file level backups
- Management of network devices
- Migrating VMs on or off the platform

Third-Party Utilities and Applications

- Management of third-party enhancement tools, utilities or applications

Minimum Requirements

For each Protected VM:

- Subscription to Company Managed Services for VM DR administration
- Size the Protected VM to meet the specifications of the VM-GPM as defined above

For each recovery site:

- Provide a Replication Network
- Provide firewall

Security of all Client environments (unless specifically subscribed to Company provided security services)

Business Continuity / Disaster Recovery Plan

A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation following a disaster or interruption in business.

DR configuration activities including but not limited to the following:

- DR recovery retention window
- Server startup sequencing and startup delay
- Network mapping
- Reconfiguration of server IP address (re-IP) plan (if applicable)

Applications and Client-Side DR Configuration and Testing:

- Maintain DR test and failover procedures for all databases and applications existing on the servers included in the DR plan
- Database and application management and reconfiguration during DR testing or failover
- Configuration of end-user devices and/or Client infrastructure required to allow end users to access the environment
- Conducting functional and data validation testing during server failover testing

601727 ReliaCloud ELASTIC Protected VM-GPL

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System

Availability Zone: A location to which one can replicate VM data for protection, represented by a Prism Central instance to which a Nutanix Cluster is registered

Cluster: A logical grouping of Nodes and software to form an IT services entity

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Primary VM: A VM that is the primary source of where a production workload is run. It is also the source VM from which Snapshots are taken

Protected VM: The Primary VM that is designated to be protected by the ReliaCloud ELASTIC Protected VM service. The Primary VM resides on the Client s Nutanix AOS-based AHV Cluster, which is a separate Availability Zone and/or location from the ReliaCloud ELASTIC service environment.

Protection Policy: A combination of scheduled and configurable parameters that define how often a Snapshot of a VM is taken, how long the Snapshot is retained for, and where the Snapshot is stored

Replication Network: A network connection between the primary and recovery sites with sufficient bandwidth to accommodate the RPO requirements

RPO: Recovery Point Objective: The targeted maximum amount of data that will be unavailable in the Disaster Recovery (DR) system in terms of time, backwards from the point of disaster.

Snapshot: A point in time copy of a VM which is facilitated by the hypervisor

VM: Virtual machine

Company's Responsibilities and Included Features

ReliaCloud ELASTIC Protected VM-GPL (VM-GPL) service is comprised of compute resources which includes storage space for replicated Snapshots and the ability to power on, run, and operate the replicated VM at Client s discretion. This service is applied to a single Primary VM that meets the compute sizing specifications of the VM-GPL listed below.

VM-GPL specifications

The VM-GPL is designed as a general-purpose performance VM. Company will provide compute resources for a Primary VM with the following specifications:

- 4 vCPU
- 12GB RAM
- 80 GB O/S Drive
- 500 GB Data Drive

Protection of the Primary VM includes:

- Creation of protection policy(ies) based on Client-provided objectives (collectively Protection Policy)
- Application of the Protection Policy to the Primary VM
- Execution of the Protection Policy
- Replication of Snapshots of the Protected VM to Company s ReliaCloud ELASTIC Cluster at an interval determined by Client and Company and then applied by Company

Powered-On / Powered-Off Status

Protected VMs are replicated to the ReliaCloud ELASTIC Cluster in a powered-off state and remain powered off until powered on. In order to utilize the replicated VM, Client must request Company power the VM on. Client may request the replicated VM to be powered on for testing, fail-over, long-term production or other purposes. During a fail-over event, replication services will not be available until another fail-over or fail-back target is agreed to by Company and Client and setup by Company to restart replication services.

Service Metering

- This Service is a metered service
- The Service is billed against each Protected VM that matches the specifications of the VM-GPL
- The existence of the Protected VM s data within the ReliaCloud ELASTIC cluster will count towards the number of VMs being billed that month. The existence of the Protected VM s data will count towards service billing regardless of the VM s powered state.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Approval of Company-provided Protection Policy
- Notify Company of any requirements or modifications requested to the Services
- Application licensing and supporting maintenance including the hypervisor (if not AHV),VM operating system licensing and support maintenance.
- All file system or file level backups
- Management of network devices
- Migrating VMs on or off the platform

Third-Party Utilities and Applications

- Management of third-party enhancement tools, utilities or applications

Minimum Requirements

For each Protected VM:

- Subscription to Company Managed Services for VM DR administration
- Size the Protected VM to meet the specifications of the VM-GPL as defined above

For each recovery site:

- Provide a Replication Network
- Provide firewall

Security of all Client environments (unless specifically subscribed to Company provided security services)

Business Continuity / Disaster Recovery Plan

A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation following a disaster or

interruption in business.

DR configuration activities including but not limited to the following:

- DR recovery retention window
- Server startup sequencing and startup delay
- Network mapping
- Reconfiguration of server IP address (re-IP) plan (if applicable)

Applications and Client-Side DR Configuration and Testing:

- Maintain DR test and failover procedures for all databases and applications existing on the servers included in the DR plan
- Database and application management and reconfiguration during DR testing or failover
- Configuration of end-user devices and/or Client infrastructure required to allow end users to access the environment
- Conducting functional and data validation testing during server failover testing

601728 ReliaCloud ELASTIC Protected VM-GPXL

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System

Availability Zone: A location to which one can replicate VM data for protection, represented by a Prism Central instance to which a Nutanix Cluster is registered

Cluster: A logical grouping of Nodes and software to form an IT services entity

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Primary VM: A VM that is the primary source of where a production workload is run. It is also the source VM from which Snapshots are taken

Protected VM: The Primary VM that is designated to be protected by the ReliaCloud ELASTIC Protected VM service. The Primary VM resides on the Client s Nutanix AOS-based AHV Cluster, which is a separate Availability Zone and/or location from the ReliaCloud ELASTIC service environment.

Protection Policy: A combination of scheduled and configurable parameters that define how often a Snapshot of a VM is taken, how long the Snapshot is retained for, and where the Snapshot is stored

Replication Network: A network connection between the primary and recovery sites with sufficient bandwidth to accommodate the RPO requirements

RPO: Recovery Point Objective: The targeted maximum amount of data that will be unavailable in the Disaster Recovery (DR) system in terms of time, backwards from the point of disaster.

Snapshot: A point in time copy of a VM which is facilitated by the hypervisor

VM: Virtual machine

Company's Responsibilities and Included Features

ReliaCloud ELASTIC Protected VM-GPXL (VM-GPXL) service is comprised of compute resources which includes storage space for replicated Snapshots and the ability to power on, run, and operate the replicated VM at Client s discretion. This service is applied to a single Primary VM that meets the compute sizing specifications of the VM-GPXL listed below.

VM-GPXL specifications

The VM-GPXL is designed as a general-purpose performance VM. Company will provide compute resources for a Primary VM with the following specifications:

- 8 vCPU
- 16 GB RAM
- 80 GB O/S Drive
- 1000 GB Data Drive

Protection of the Primary VM includes:

- Creation of protection policy(ies) based on Client-provided objectives (collectively Protection Policy)
- Application of the Protection Policy to the Primary VM
- Execution of the Protection Policy
- Replication of Snapshots of the Protected VM to Company s ReliaCloud ELASTIC Cluster at an interval determined by Client and Company and then applied by Company

Powered-On / Powered-Off Status

Protected VMs are replicated to the ReliaCloud ELASTIC Cluster in a powered-off state and remain powered off until powered on. In order to utilize the replicated VM, Client must request Company power the VM on. Client may request the replicated VM to be powered on for testing, fail-over, long-term production or other purposes. During a fail-over event, replication services will not be available until another fail-over or fail-back target is agreed to by Company and Client and setup by Company to restart replication services.

Service Metering

- This Service is a metered service
- The Service is billed against each Protected VM that matches the specifications of the VM-GPXL
- The existence of the Protected VM s data within the ReliaCloud ELASTIC cluster will count towards the number of VMs being billed that month. The existence of the Protected VM s data will count towards service billing regardless of the VM s powered state.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Approval of Company-provided Protection Policy
- Notify Company of any requirements or modifications requested to the Services
- Application licensing and supporting maintenance including the hypervisor (if not AHV),VM operating system licensing and support maintenance.
- All file system or file level backups
- Management of network devices
- Migrating VMs on or off the platform

Third-Party Utilities and Applications

- Management of third-party enhancement tools, utilities or applications

Minimum Requirements

For each Protected VM:

- Subscription to Company Managed Services for VM DR administration
- Size the Protected VM to meet the specifications of the VM-GPXL as defined above

For each recovery site:

- Provide a Replication Network
- Provide firewall

Security of all Client environments (unless specifically subscribed to Company provided security services)

Business Continuity / Disaster Recovery Plan

A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation following a disaster or interruption in business.

DR configuration activities including but not limited to the following:

- DR recovery retention window
- Server startup sequencing and startup delay
- Network mapping
- Reconfiguration of server IP address (re-IP) plan (if applicable)

Applications and Client-Side DR Configuration and Testing:

- Maintain DR test and failover procedures for all databases and applications existing on the servers included in the DR plan
- Database and application management and reconfiguration during DR testing or failover
- Configuration of end-user devices and/or Client infrastructure required to allow end users to access the environment
- Conducting functional and data validation testing during server failover testing

601729 ReliaCloud ELASTIC Protected VM-GP2XL

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System

Availability Zone: A location to which one can replicate VM data for protection, represented by a Prism Central instance to which a Nutanix Cluster is registered

Cluster: A logical grouping of Nodes and software to form an IT services entity

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Primary VM: A VM that is the primary source of where a production workload is run. It is also the source VM from which Snapshots are taken

Protected VM: The Primary VM that is designated to be protected by the ReliaCloud ELASTIC Protected VM service. The Primary VM resides on the Client s Nutanix AOS-based AHV Cluster, which is a separate Availability Zone and/or location from the ReliaCloud ELASTIC service environment.

Protection Policy: A combination of scheduled and configurable parameters that define how often a Snapshot of a VM is taken, how long the Snapshot is retained for, and where the Snapshot is stored

Replication Network: A network connection between the primary and recovery sites with sufficient bandwidth to accommodate the RPO requirements

RPO: Recovery Point Objective: The targeted maximum amount of data that will be unavailable in the Disaster Recovery (DR) system in terms of time, backwards from the point of disaster.

Snapshot: A point in time copy of a VM which is facilitated by the hypervisor

VM: Virtual machine

Company's Responsibilities and Included Features

ReliaCloud ELASTIC Protected VM-GP2XL (VM-GP2XL) service is comprised of compute resources which includes storage space for replicated Snapshots and the ability to power on, run, and operate the replicated VM at Client s discretion. This service is applied to a single Primary VM that meets the compute sizing specifications of the VM-GP2XL listed below.

VM-GP2XL specifications

The VM-GP2XL is designed as a general-purpose performance VM. Company will provide compute resources for a Primary VM with the following specifications:

- 8 vCPU
- 32 GB RAM
- 80 GB O/S Drive
- 1500 GB Data Drive

Protection of the Primary VM includes:

- Creation of protection policy(ies) based on Client-provided objectives (collectively Protection Policy)
- Application of the Protection Policy to the Primary VM
- Execution of the Protection Policy
- Replication of Snapshots of the Protected VM to Company s ReliaCloud ELASTIC Cluster at an interval determined by Client and Company and then applied by Company

Powered-On / Powered-Off Status

Protected VMs are replicated to the ReliaCloud ELASTIC Cluster in a powered-off state and remain powered off until powered on. In order to utilize the replicated VM, Client must request Company power the VM on. Client may request the replicated VM to be powered on for testing, fail-over, long-term production or other purposes. During a fail-over event, replication services will not be available until another fail-over or fail-back target is agreed to by Company and Client and setup by Company to restart replication services.

Service Metering

- This Service is a metered service
- The Service is billed against each Protected VM that matches the specifications of the VM-GP2XL
- The existence of the Protected VM s data within the ReliaCloud ELASTIC cluster will count towards the number of VMs being billed that month. The existence of the Protected VM s data will count towards service billing regardless of the VM s powered state.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request

support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Approval of Company-provided Protection Policy
- Notify Company of any requirements or modifications requested to the Services
- Application licensing and supporting maintenance including the hypervisor (if not AHV),VM operating system licensing and support maintenance.
- All file system or file level backups
- Management of network devices
- Migrating VMs on or off the platform

Third-Party Utilities and Applications

- Management of third-party enhancement tools, utilities or applications

Minimum Requirements

For each Protected VM:

- Subscription to Company Managed Services for VM DR administration
- Size the Protected VM to meet the specifications of the VM-GP2XL as defined above

For each recovery site:

- Provide a Replication Network
- Provide firewall

Security of all Client environments (unless specifically subscribed to Company provided security services)

Business Continuity / Disaster Recovery Plan

A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation following a disaster or interruption in business.

DR configuration activities including but not limited to the following:

- DR recovery retention window
- Server startup sequencing and startup delay
- Network mapping
- Reconfiguration of server IP address (re-IP) plan (if applicable)

Applications and Client-Side DR Configuration and Testing:

- Maintain DR test and failover procedures for all databases and applications existing on the servers included in the DR plan
- Database and application management and reconfiguration during DR testing or failover
- Configuration of end-user devices and/or Client infrastructure required to allow end users to access the environment
- Conducting functional and data validation testing during server failover testing

601730 ReliaCloud ELASTIC Protected VM-GP3XL

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System

Availability Zone: A location to which one can replicate VM data for protection, represented by a Prism Central instance to which a Nutanix Cluster is registered

Cluster: A logical grouping of Nodes and software to form an IT services entity

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Primary VM: A VM that is the primary source of where a production workload is run. It is also the source VM from which Snapshots are taken

Protected VM: The Primary VM that is designated to be protected by the ReliaCloud ELASTIC Protected VM service. The Primary VM resides on the Client s Nutanix AOS-based AHV Cluster, which is a separate Availability Zone and/or location from the ReliaCloud ELASTIC service environment.

Protection Policy: A combination of scheduled and configurable parameters that define how often a Snapshot of a VM is taken, how long the Snapshot is retained for, and where the Snapshot is stored

Replication Network: A network connection between the primary and recovery sites with sufficient bandwidth to accommodate the RPO requirements

RPO: Recovery Point Objective: The targeted maximum amount of data that will be unavailable in the Disaster Recovery (DR) system in terms of time, backwards from the point of disaster.

Snapshot: A point in time copy of a VM which is facilitated by the hypervisor

VM: Virtual machine

Company's Responsibilities and Included Features

ReliaCloud ELASTIC Protected VM-GP3XL (VM-GP3XL) service is comprised of compute resources which includes storage space for replicated Snapshots and the ability to power on, run, and operate the replicated VM at Client s discretion. This service is applied to a single Primary VM that meets the compute sizing specifications of the VM-GP3XL listed below.

VM-GP3XL specifications

The VM-GP3XL is designed as a general-purpose performance VM. Company will provide compute resources for a Primary VM with the following specifications:

- 8 vCPU
- 64 GB RAM
- 80 GB O/S Drive
- 2000 GB Data Drive

Protection of the Primary VM includes:

- Creation of protection policy(ies) based on Client-provided objectives (collectively Protection Policy)
- Application of the Protection Policy to the Primary VM
- Execution of the Protection Policy
- Replication of Snapshots of the Protected VM to Company s ReliaCloud ELASTIC Cluster at an interval determined by Client and Company and then applied by Company

Powered-On / Powered-Off Status

Protected VMs are replicated to the ReliaCloud ELASTIC Cluster in a powered-off state and remain powered off until powered on. In order to utilize the replicated VM, Client must request Company power the VM on. Client may request the replicated VM to be powered on for testing, fail-over, long-term production or other purposes. During a fail-over event, replication services will not be available until another fail-over or fail-back target is agreed to by Company and Client and setup by Company to restart replication services.

Service Metering

- This Service is a metered service
- The Service is billed against each Protected VM that matches the specifications of the VM-GP3XL
- The existence of the Protected VM s data within the ReliaCloud ELASTIC cluster will count towards the number of VMs being billed that month. The existence of the Protected VM s data will count towards service billing regardless of the VM s powered state.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Approval of Company-provided Protection Policy
- Notify Company of any requirements or modifications requested to the Services
- Application licensing and supporting maintenance including the hypervisor (if not AHV),VM operating system licensing and support maintenance.
- All file system or file level backups
- Management of network devices
- Migrating VMs on or off the platform

Third-Party Utilities and Applications

- Management of third-party enhancement tools, utilities or applications

Minimum Requirements

For each Protected VM:

- Subscription to Company Managed Services for VM DR administration
- Size the Protected VM to meet the specifications of the VM-GP3XL as defined above

For each recovery site:

- Provide a Replication Network
- Provide firewall

Security of all Client environments (unless specifically subscribed to Company provided security services)

Business Continuity / Disaster Recovery Plan

A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation following a disaster or interruption in business.

DR configuration activities including but not limited to the following:

- DR recovery retention window
- Server startup sequencing and startup delay

- Network mapping
- Reconfiguration of server IP address (re-IP) plan (if applicable)

Applications and Client-Side DR Configuration and Testing:

- Maintain DR test and failover procedures for all databases and applications existing on the servers included in the DR plan
- Database and application management and reconfiguration during DR testing or failover
- Configuration of end-user devices and/or Client infrastructure required to allow end users to access the environment
- Conducting functional and data validation testing during server failover testing

Category: Security

110032 Enterprise Firewall Service

Company's Responsibilities and Included Features

The enterprise firewall service provides a dedicated security service instance (context) that lives across highly available redundant hardware. The service is ideally targeted for Clients within ReliaCloud Public or Private. The service is also applicable to colocation Clients that desire to outsource their security services layer.

- Dedicated security service instance (context)
- Highly available redundant hardware
- Up To 5 Security Segments. 1 outside plus up to 4 additional segments
- 500 maximum firewall access rules
- Up to 8000 sessions per second
- Maintaining firewall operation including current and best supported service version
- Defining and applying security best practices
- All service context configuration activities, including configuration updates and port openings/closures
- Monitoring and reporting of key metrics including port availability, interface utilization, and overall ASA/firewall health/availability
- Bandwidth utilization reporting and trending
- Syslog alerting and archiving
- IOS/OS issue resolution and triage
- IOS/OS patch/upgrade management
- Includes weekly reviews of needed critical patches and updates during approved maintenance windows
- Port assignments and configuration
- VLAN assignment management and tracking
- Daily configuration backups of network device with change log
- Firewall maintenance including management of firewall rules up to the service maximum
- 24/7 expert-to-expert engineering support
- Up to 4 Contexts can be stacked together to form a larger service unit

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of any service requirements, changes or modifications

600229 ASAv VPN Base Service

Company's Responsibilities and Included Features

- Up-to 250 customer Cisco AnyConnect users

- Using a throughput of 50 mbps or less (aggregate; actual Internet bandwidth usage is not included in this SKU)
- Using 100,000 or fewer concurrent connections
- Maintain the ASAv as a fully-managed and monitored appliance, with the exception of per-user certificate generation, per-user authentication, and per-user support (see Client Responsibilities)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Designate a network segment (VLAN) within the Client's ReliaCloud environment, on which to connect the ASAv appliance
- Additional charges may apply if an additional VLAN is needed, and is not available within the Client's existing ReliaCloud resource allocation.
- Provide or contract for the ASAv's access to the Internet, if the designated network segment does not already have Internet access
- Designate a syslog server within the Client's ReliaCloud environment, to which the VPN appliance should log per-user VPN session information (optional)
- Configure per-user authentication
- Provision per-user certificates using the ASAv for certificate-based two-factor authentication (optional; instructions and support provided)
- Maintain per-user authentication (required), such as:
    - Designate an Active Directory/LDAP, TACACS or RADIUS server within the Client's ReliaCloud environment to be used for per-user authentication; or else configure and maintain per-user accounts within the ASAv virtual applianceconfiguration

600230 ASAv Per User VPN

Company's Responsibilities and Included Features

Provide per user VPN connectivity via ASAv

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Subscribe to 600229 ASAv VPN Base Service

600623 Desktop Virus Control - 20 device minimum

Company's Responsibilities and Included Features

Centralized virus control for desktops associated with a managed IT environment includes:

- License, maintain, and support anti-virus (AV) software.
- Provide automatic updates to virus control pattern files.
- Report virus trending and compliance.
- Provide Client IT personnel a Client software install point for desktop roll-out.
- Provide reasonable efforts to contain and manage virus outbreaks and provide priority alerts to Client contacts.
- Provide automatic roll-out of AV software and updates.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide Company mutually-agreed upon access to Client s desktops/laptops covered by this Service with AV remote hands for desk-side support issues related to the implementation and management of this service.
- Implement and maintain virus control procedures for inbound email.
- Provide end user support for all applications and components other than AV software components covered by this service.

601528 Managed Hosted Cisco Firewall Service - Cisco ASA 5516-x Pair with FirePOWER

Company's Responsibilities and Included Features

Provide a Cisco firewall pair (2 devices) with FirePOWER (hereinafter the Device) services on a monthly subscription basis. The Service will be hosted from within a Company data center, and includes the following features*:

- Cisco ASA High Availability (HA) pair hardware based
- FirePOWER software
- Support for strong encryption (3DES/AES)
- Support for up to 5 security contexts
- Support for up to 100 simultaneous Cisco AnyConnect VPNs
- 8 gigabit Ethernet interfaces
- Up to 850 Mbps throughput Application Visibility Control (AVC)
- Up to 450 Mbps throughput AVC and Intrusion Prevention System (IPS)
- Up to 250,000 concurrent sessions
- Up to 20,000 new connections per second

Firewall Hosting

- Provide a secure four-sided locking cabinet to host the Device. Cabinets are multi-tenant and are under the exclusive control of Company
- Provide continuous power to the Device via A and B side power feeds
- Ensure proper power load distribution across A and B power feeds
- Maintain appropriate environmental standards for HVAC consistent with equipment manufacturing recommendations
- Maintain physical security of the cabinet
- Provide all physical moves, adds, and changes
- Provide primary and redundant network connections
- No physical or administrative configuration access to the Device will be granted to Client

Firewall Management

- Address translation (NAT/PAT)
- Firewall rule management
- Cluster configuration (if needed)
- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support; Cisco client based or AnyConnect is not supported when firewall is contextualized
    - Supports local DB and DLAP authentication
- Hardware maintenance management
    - Manage hardware replacement and/or repair with hardware vendor
    - Perform analysis of any hardware additions or upgrades
    - Apply hardware IOS\OS updates as necessary
- Remote access VPN management
    - Deployment and support of client based remote access VPN including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management

        - Client VPN access utilizing Cisco client software
        - Limited to twenty (20) named users if local device authentication is used
    - Site-to-site VPN management
        - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
        - Troubleshooting / support of VPN tunnel establishment

FirePOWER IPS (Intrusion Prevention System) Support

- Support and troubleshoot perimeter intrusion prevention (at Internet boundary/ingress)
- Support and troubleshoot cross site scripting, basic intrusion detection (ingress/egress)
- Minor tuning management, limited to IPS/IDS (Intrusion Detection System) feature set
- Update Cisco FirePOWER application signatures
- Configuration and delivery of Cisco FirePOWER standard reports (non-custom)
- Confirm that reports and alerts are functioning
- Schedule standard Cisco FirePOWER reports and alerts
- Troubleshoot alerts related to Company managed applications and devices
- Configuration of SIEM (Security Incident Event Management) integration (SIEM service is out of scope)
- Manage hardware replacement and or repair with hardware vendor

*Company may substitute alternative products with similar features and functionality at Company s sole discretion

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

SIEM services

- Perform Security Operations Center (SOC) services including but not limited to:
    - Security incident response
    - Security incident identification, analysis, defense, investigation and reporting
    - Data breach investigation and reporting
    - Security gap analysis
    - Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Managed Cisco Firewall Service High Availability Pair service is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html.

601766 Managed Cisco Adaptive Security Virtual Appliance (ASAv10)

The Managed Cisco Adaptive Security Virtual Appliance Model 10 (Managed ASAv10) service is a combination of Company managed services for a firewall and Cisco software licensing for the purpose of running a single (non-redundant) ASAv10 firewall on virtualized infrastructure provided by Client or contracted to be provided by Company.

Definitions

Intellectual Property: any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Feature Specification

The following table provides the ASAv10 feature specifications that Company will manage:

Feature	Entitlement / Managed Support	Licensing Included
Stateful inspection firewall throughput (maximum) *	1 Gbps	Yes
Stateful inspection firewall throughput (multiprotocol) **	500 Mbps	Yes
Advanced Encryption Standard (AES) VPN throughput***	750 Mbps	Yes
Connections per second	20,000	Yes
Concurrent sessions	100,000	Yes
VLANs	50	Yes
Bridge groups	25	Yes
IPsec VPN peers****	25	Yes
Cisco AnyConnect or clientless VPN user sessions*****	250	Yes

Note: Cisco s Cisco Adaptive Security Virtual Appliance v10 may include software features not listed in the table above. Any unlisted services are not within the scope of Company s managed support of virtual appliance.

*Maximum throughput measured by Cisco with User Datagram Protocol (UDP) traffic under ideal conditions.

** Multiprotocol refers to a traffic profile consisting primarily of TCP-based protocols or applications like HTTP, SMTP, FTP, IMAPv4, BitTorrent, and DNS.

*** The VPN throughput and the number of sessions depend on the ASA device configuration and VPN traffic patterns. These elements should be taken into consideration as part of your capacity planning.

**** Note, additional IPSec VPN peers (>25) are available and can be purchased from Company under a separate ItemID.

*****Cisco AnyConnect or clientless VPN user sessions are not included with this ItemID, but can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Firewall Management

- Configuration of address translation (NAT/PAT)
- Configuration of firewall rule management
- Virtualization cluster configuration support (if needed)
- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of Cisco AnyConnect including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing Cisco client software

Site-to-site VPN management

- Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
- Troubleshooting / support of VPN tunnel establishment

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the ASAv5 software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

End of Support

The Cisco ASAv10 is subject to an EOS Date, as described above in this SOW.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Intellectual Property in and to the Services belonging to Cisco or other Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide virtualizing resources to meet or exceed the Managed ASAv10 Infrastructure specifications.
    - Minimum virtualized resources necessary to run the Managed ASAv10 are as follows:
        - 2 vCPU
        - 4 GB memory *
        - 8 GB storage

  * Up to 8 GB of memory is required to support 50 Cisco AnyConnect User Sessions

- Provide and configure desired internal and external network services

- Open any necessary ports and conduits between the Appliance and Company s management services
- Specify and implement, desired fault tolerance. Note, the Managed ASAv10 is a single (1) virtual appliance and non-redundant. Should Client desire fault tolerance from a fail-over, reboot, or system maintenance window, a second (2 total) Managed ASAv10 should be deployed and configured for high-availability. That service is available from Company under a separate ItemID.
- Client is responsible for performing all Security Operations Center (SOC) services including but not limited to:
    - Security incident response
    - Security incident identification, analysis, defense, investigation and reporting
    - Data breach investigation and reporting
    - Security gap analysis
    - Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco ASAv10 software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf and the Cisco Secure Supplemental End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/anyconnect-SEULA-v4x.pdf (collectively the Cisco Terms).

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at OneNeck or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Intellectual Property rights including pursuing an action against any breaching third parties.

601767 Managed Cisco Adaptive Security Virtual Appliance (ASAv30)

The Managed Cisco Adaptive Security Virtual Appliance Model 30 (Managed ASAv30) service is a combination of Company managed services for a firewall and Cisco software licensing for the purpose of running a single (non-redundant) ASAv30 firewall on virtualized infrastructure provided by Client or contracted to be provided by Company.

Definitions

Intellectual Property: any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Feature Specification

The following table provides the ASAv30 feature specifications that Company will manage:

Feature	Entitlement / Managed Support	Licensing Included
Stateful inspection firewall throughput (maximum) *	2 Gbps	Yes
Stateful inspection firewall throughput (multiprotocol) **	1 Gbps	Yes
Advanced Encryption Standard (AES) VPN throughput***	2 Gbps	Yes
Connections per second	60,000	Yes

Concurrent sessions	500,000	Yes
VLANs	200	Yes
Bridge groups	100	Yes
IPsec VPN peers****	25	Yes
Cisco AnyConnect or clientless VPN user sessions*****	750	Yes

Note: Cisco s Cisco Adaptive Security Virtual Appliance v30 may include software features not listed in the table above. Any unlisted services are not within the scope of Company s managed support of virtual appliance.

*Maximum throughput measured by Cisco with User Datagram Protocol (UDP) traffic under ideal conditions.

** Multiprotocol refers to a traffic profile consisting primarily of TCP-based protocols or applications like HTTP, SMTP, FTP, IMAPv4, BitTorrent, and DNS.

*** The VPN throughput and the number of sessions depend on the ASA device configuration and VPN traffic patterns. These elements should be taken into consideration as part of your capacity planning.

**** Note, additional IPSec VPN peers (>25) are available and can be purchased from Company under a separate ItemID.

*****Cisco AnyConnect or clientless VPN user sessions are not included with this ItemID, but can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Firewall Management

- Configuration of address translation (NAT/PAT)
- Configuration of firewall rule management
- Virtualization cluster configuration support (if needed)
- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of Cisco AnyConnect including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing Cisco client software
    - Site-to-site VPN management
        - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
        - Troubleshooting / support of VPN tunnel establishment

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the ASAv5 software (including major upgrades) will be conducted at Company s discretion and in

accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

End of Support

The Cisco ASAv30 is subject to an EOS Date, as described above in this SOW.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Intellectual Property in and to the Services belonging to Cisco or other Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide virtualizing resources to meet or exceed the Managed ASAv30 Infrastructure specifications.
    - Minimum virtualized resources necessary to run the Managed ASAv30 are as follows:
        - 4 vCPU
        - 8 GB memory *
        - 8 GB storage

  * Up to 8 GB of memory is required to support 50 Cisco AnyConnect User Sessions

- Provide and configure desired internal and external network services
- Open any necessary ports and conduits between the Appliance and Company s management services
- Specify and implement, desired fault tolerance. Note, the Managed ASAv30 is a single (1) virtual appliance and non-redundant. Should Client desire fault tolerance from a fail-over, reboot, or system maintenance window, a second (2 total) Managed ASAv30 should be deployed and configured for high-availability. That service is available from Company under a separate ItemID.
- Client is responsible for performing all Security Operations Center (SOC) services including but not limited to:
    - Security incident response
    - Security incident identification, analysis, defense, investigation and reporting
    - Data breach investigation and reporting
    - Security gap analysis

Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco ASAv30 software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf and the Cisco Secure Supplemental End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/anyconnect-SEULA-v4x.pdf (collectively the Cisco Terms).

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at OneNeck or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Intellectual Property rights including pursuing an action against any breaching third parties.

601775 Managed Cisco Adaptive Security Virtual Appliance (ASAv5) HA Pair

The Managed Cisco Adaptive Security Virtual Appliance ASAv5 HA (Managed ASAv5 HA) service is a combination of Company managed services for a pair of ASAv5s deployed in a high availability configuration (active/standby) and Cisco software licensing for the purpose of running a Managed ASAv5 HA firewall on virtualized infrastructure provided by Client or contracted to be provided by Company.

Definitions

Intellectual Property: any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Feature Specification

The following table provides the ASAv5 feature specifications that Company will manage:

Feature	**Entitlement / Managed Support**	**Licensing Included**
Stateful inspection firewall throughput (maximum) *	100 Mbps	Yes
Stateful inspection firewall throughput (multiprotocol) **	50 Mbps	Yes
Advanced Encryption Standard (AES) VPN throughput***	30 Mbps	Yes
Connections per second	8,000	Yes
Concurrent sessions	50,000	Yes
VLANs	25	Yes
Bridge groups	12	Yes
IPsec VPN peers****	25	Yes
Cisco AnyConnect or clientless VPN user sessions*****	50	Yes

Note: Cisco s Cisco Adaptive Security Virtual Appliance v5 may include software features not listed in the table above. Any unlisted services are not within the scope of Company s managed support of virtual appliance.

*Maximum throughput measured by Cisco with User Datagram Protocol (UDP) traffic under ideal conditions.

** Multiprotocol refers to a traffic profile consisting primarily of TCP-based protocols or applications like HTTP, SMTP, FTP, IMAPv4, BitTorrent, and DNS.

*** The VPN throughput and the number of sessions depend on the ASA device configuration and VPN traffic patterns. These elements should be taken into consideration as part of your capacity planning.

**** Note, additional IPSec VPN peers (>25) are available and can be purchased from Company under a separate ItemID.

*****Cisco AnyConnect or clientless VPN user sessions are not included with this ItemID, but can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Firewall Management

- Configuration of address translation (NAT/PAT)
- Configuration of firewall rule management
- Virtualization cluster configuration support (if needed)
- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of Cisco AnyConnect including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing Cisco client software
    - Site-to-site VPN management
        - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
        - Troubleshooting / support of VPN tunnel establishment

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the ASAv5 software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

End of Support

The Cisco ASAv5 is subject to an EOS Date, as described above in this SOW.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Intellectual Property in and to the Services belonging to Cisco or other Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide virtualizing resources to meet or exceed the Managed ASAv5 Infrastructure specifications.
    - Combined minimum virtualized resources necessary to run the Managed ASAv5 HA pair are as follows:
        - 2 vCPU
        - 4 GB memory *
        - 16 GB storage

  * Up to 8 GB of memory is required to support 50 Cisco AnyConnect User Sessions

- Provide and configure desired internal and external network services
- Open any necessary ports and conduits between the Appliance and Company s management services
- Client is responsible for performing all Security Operations Center (SOC) services including but not limited to:
    - Security incident response
    - Security incident identification, analysis, defense, investigation and reporting
    - Data breach investigation and reporting
    - Security gap analysis
    - Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco ASAv5 software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf and the Cisco Secure Supplemental End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/anyconnect-SEULA-v4x.pdf (collectively the Cisco Terms).

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and

further agrees that it will, at OneNeck or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Intellectual Property rights including pursuing an action against any breaching third parties.

601853 Cisco Secure Endpoint Licenses (formerly called Cisco AMP for Endpoints)

Cisco Secure Endpoint is a cloud-based advanced malware analysis and protection solution that allows users to conduct metadata file analysis to detect malware and cyber threats.

Notwithstanding the Term of this Statement of Work, this Service is provided for a minimum of 12 months. Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Definitions

Endpoint(s): any device capable of processing data and that can access a network, including but not limited to personal computers, mobile devices and network computer workstations.

Intellectual Property: any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Company's Responsibilities and Included Features

Licenses

Provide Cisco Secure Endpoint Licenses up to the quantity as stated in the Pricing Details above. Endpoint Licenses will be provided on a monthly subscription basis and must be implemented and deployed prior to use by Client.

- License Restrictions. This ItemID provides a license, not a transfer of title, to the Cisco Secure Endpoint Licenses. Cisco retains ownership of all copies of the Cisco Secure Endpoint License and related software and documentation. Client acknowledges that the Cisco Secure Endpoint software and documentation contain trade secrets of Cisco, its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Unless expressly authorized in writing by Cisco or otherwise permitted under applicable law, Client will not:
    - a. sell, resell, transfer, sublicense, or assign its license rights under this SOW;
    - b. modify, adapt or create derivative works;
    - c. reverse engineer, decompile, decrypt, disassemble or otherwise attempt to derive source code;
    - d. Use the Cisco Secure Endpoint software that is licensed for a specific device, whether physical or virtual, on another device;
    - e. remove, modify, or conceal any product identification, copyright, proprietary, intellectual property notices or other marks;
    - f. Use the Cisco Secure Endpoint software on secondhand or refurbished Cisco equipment not authorized by Cisco;
    - g. locate the Cisco Secure Endpoint software in Brazil, Russia, India and/or mainland China, unless mutually agreed in writing by the parties and authorized by Cisco;
    - h. Use any Cisco provided content or data other than with the Cisco Secure Endpoint software and any third-party products or services that Cisco has identified as compatible with the Cisco Secure Endpoint software

Service Metering

- This is a metered service billed in arrears on a monthly basis.
- Endpoints connected to the Cisco Secure Endpoint Cloud for 16 days or more in the previous month are billable for the full month. Endpoints used for 15 days or fewer in a given month will not be charged for that month.
- Company may back bill Client for any error that results in an under-billing to Client within 180 days of the issuance of

the invoice that should have reflected the under-billed usage. If Client has any reason to dispute an invoice, Client must notify Company in writing of any such disputed fees within 10 days of the invoice date and provide OneNeck with written details about why Client disputes the invoice.

Cisco Threat Response. Secure Endpoint includes access to Cisco Threat Response. Please see the Cisco Threat Response Privacy Data Sheet (https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=Privacy%20Data%20Sheet|Privacy%20Data%20Map) regarding any personal data processed by Cisco Threat Response. .

Cisco Secure Endpoint Portal Setup

- Setup Client web portal (AMP for Endpoints dashboard)

Cisco Secure Endpoint Support Services

- Upon Client request, escalate appropriate issues to Cisco TAC (Technical Assistance Center)

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Intellectual Property in and to the Services belonging to Cisco or other Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party.

Warranties. NEITHER COMPANY NOR CISCO REPRESENT OR WARRANT THAT THE MANAGED CISCO AMP FOR ENDPOINTS LICENSES AND/OR SUPPORT SERVICE WILL GUARANTEE ABSOLUTE SECURITY DUE TO THE CONTINUAL DEVELOPMENT OF NEW TECHNIQUES FOR INTRUDING UPON AND ATTACKING FILES, NETWORKS AND ENDPOINTS. NEITHER COMPANY NOR CISCO REPRESENT OR WARRANT THAT THE CLOUD SERVICES WILL PROTECT ALL OF CLIENT S FILES, NETWORK, OR ENDPOINTS FROM ALL MALWARE, VIRUSES OR THIRD- PARTY MALICIOUS ATTACKS. NEITHER COMPANY NOR CISCO MAKE ANY REPRESENTATIONS OR WARRANTIES REGARDING ANY THIRD-PARTY SYSTEM OR SERVICE TO WHICH THIS MANAGED CISCO AMP FOR ENDPOINTS AND SUPPORT SERVICE INTEGRATES OR TO ANY ONGOING INTEGRATION SUPPORT. INTEGRATIONS MADE ACCESSIBLE TO CLIENT THAT ARE NOT A GENERALLY AVAILABLE PRODUCT INCLUDED ON YOUR ORDER ARE PROVIDED ON AN "AS IS" BASIS.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless contracted separately with Company under this or another Executed Order, Client is responsible for the following:

- Implementation and deployment are not included in this ItemID, and must be contracted separately with Company. Client may not use Secure Endpoint Licenses which have not been implemented and deployed.
- When assigning any names (policy, group, exclusion, etc.) with the exception of Computer name, Client may not use ON- at the beginning of the name. The ON- designation is reserved for Company usage only.
- Notify Company of any Cisco Secure Endpoint service issues
- Allow access to any devices to be connected to Secure Endpoint software
- Allow configuration of firewall rules required for access to the Cisco Secure Endpoint Cloud
- Designate a primary Client contact for security incident escalations
- Security Incident Event Management (SIEM) services

End User License Agreement

The Cisco Secure Endpoint service is subject to the applicable Cisco End User License Agreement located at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco EULA"). Client acknowledges and accepts that its subscription to and use of this Service is subject to the Cisco Terms.

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and

further agrees that it will, at OneNeck or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Intellectual Property rights including pursuing an action against any breaching third parties.

601909 ASAv30 VPN Connectivity Licenses For 25 User Sessions

Company's Responsibilities and Included Features

For each quantity of this ItemID subscribed to, Company will provide 25 Cisco AnyConnect Plus Licenses.

Note: The total number of Cisco AnyConnect Plus Licenses cannot exceed 750.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Current subscription for Company s Managed Cisco Adaptive Security Virtual Appliance (ASAv30).

Additional ASAv resources for CPU memory and storage may be required depending on number of additional VPN Connectivity Licenses used.

End User License Agreement

Client agrees that the Cisco ASAv30 software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf

601910 ASAv50 VPN Connectivity Licenses For 25 User Sessions

Company's Responsibilities and Included Features

For each quantity of this ItemID subscribed to, Company will provide 25 Cisco AnyConnect Plus Licenses.

Note: The total number of Cisco AnyConnect Plus Licenses cannot exceed 10,000.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Current subscription for Company s Managed Cisco Adaptive Security Virtual Appliance (ASAv50).

Additional ASAv resources for CPU memory and storage may be required depending on number of additional VPN Connectivity Licenses used.

End User License Agreement

Client agrees that the Cisco ASAv50 software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf

602178 Managed Cisco Adaptive Security Virtual Appliance (ASAv30) HA Pair

The Managed Cisco Adaptive Security Virtual Appliance ASAv30 HA (Managed ASAv30 HA) service is a combination of Company managed services for a pair of ASAv30s deployed in a high availability configuration (active/standby) and Cisco software licensing for the purpose of running a Managed ASAv30 HA firewall on virtualized infrastructure provided by Client or contracted to be provided by Company.

Definitions

Intellectual Property: any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and

however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Feature Specification

The following table provides the ASAv30 feature specifications that Company will manage:

Feature	**Entitlement / Managed Support**	**Licensing Included**
Stateful inspection firewall throughput (maximum) *	2 Gbps	Yes
Stateful inspection firewall throughput (multiprotocol) **	1 Gbps	Yes
Advanced Encryption Standard (AES) VPN throughput***	2 Gbps	Yes
Connections per second	60,000	Yes
Concurrent sessions	500,000	Yes
VLANs	200	Yes
Bridge groups	100	Yes
IPsec VPN peers****	25	Yes
Cisco AnyConnect or clientless VPN user sessions	750	Yes

Note: Cisco s Cisco Adaptive Security Virtual Appliance v30 may include software features not listed in the table above. Any unlisted services are not within the scope of Company s managed support of virtual appliance.

*Maximum throughput measured by Cisco with User Datagram Protocol (UDP) traffic under ideal conditions.

** Multiprotocol refers to a traffic profile consisting primarily of TCP-based protocols or applications like HTTP, SMTP, FTP, IMAPv4, BitTorrent, and DNS.

*** The VPN throughput and the number of sessions depend on the ASA device configuration and VPN traffic patterns. These elements should be taken into consideration as part of your capacity planning.

**** Note, additional IPSec VPN peers (>25) are available and can be purchased from Company under a separate ItemID.

*****Cisco AnyConnect or clientless VPN user sessions are not included with this ItemID, but can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Firewall Management

- Configuration of address translation (NAT/PAT)
- Configuration of firewall rule management
- Virtualization cluster configuration support (if needed)
- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)

        - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of Cisco AnyConnect including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing Cisco client software
    - Site-to-site VPN management
        - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
        - Troubleshooting / support of VPN tunnel establishment

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the ASAv30 software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

End of Support

The Cisco ASAv30 is subject to an EOS Date, as described above in this SOW.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Intellectual Property in and to the Services belonging to Cisco or other Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide virtualizing resources to meet or exceed the Managed ASAv30 Infrastructure specifications.

Combined minimum virtualized resources necessary to run the Managed ASAv30 HA pair are as follows:

- 8 vCPU
- 16 GB memory *
- 16 GB storage

* Up to 8 GB of memory is required to support 50 Cisco AnyConnect User Sessions

- Provide and configure desired internal and external network services
- Open any necessary ports and conduits between the Appliance and Company s management services
- Client is responsible for performing all Security Operations Center (SOC) services including but not limited to:
  - Security incident response
  - Security incident identification, analysis, defense, investigation and reporting
  - Data breach investigation and reporting
  - Security gap analysis
  - Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco ASAv30 software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf and the Cisco Secure Supplemental End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/anyconnect-SEULA-v4x.pdf (collectively the Cisco Terms).

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at OneNeck or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Intellectual Property rights including pursuing an action against any breaching third parties.

602179 Managed Cisco Adaptive Security Virtual Appliance (ASAv50) HA Pair

The Managed Cisco Adaptive Security Virtual Appliance ASAv50 HA (Managed ASAv50 HA) service is a combination of Company managed services for a pair of ASAv50s deployed in a high availability configuration (active/standby) and Cisco software licensing for the purpose of running a Managed ASAv50 HA firewall on virtualized infrastructure provided by Client or contracted to be provided by Company.

Definitions

Intellectual Property: any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Feature Specification

The following table provides the ASAv50 feature specifications that Company will manage:

Feature	Entitlement / Managed Support	Licensing Included
Stateful inspection firewall throughput (maximum) *	10 Gbps	Yes
Stateful inspection firewall throughput (multiprotocol) **	5 Gbps	Yes

Advanced Encryption Standard (AES) VPN throughput***	4 Gbps	Yes
Connections per second	120,000	Yes
Concurrent sessions	2,000,000	Yes
VLANs	1,024	Yes
Bridge groups	250	Yes
IPsec VPN peers****	25	Yes
Cisco AnyConnect or clientless VPN user sessions*****	10,000	Yes

Note: Cisco s Cisco Adaptive Security Virtual Appliance v50 may include software features not listed in the table above. Any unlisted services are not within the scope of Company s managed support of virtual appliance.

*Maximum throughput measured by Cisco with User Datagram Protocol (UDP) traffic under ideal conditions.

** Multiprotocol refers to a traffic profile consisting primarily of TCP-based protocols or applications like HTTP, SMTP, FTP, IMAPv4, BitTorrent, and DNS.

*** The VPN throughput and the number of sessions depend on the ASA device configuration and VPN traffic patterns. These elements should be taken into consideration as part of your capacity planning.

**** Note, additional IPSec VPN peers (>25) are available and can be purchased from Company under a separate ItemID.

*****Cisco AnyConnect or clientless VPN user sessions are not included with this ItemID, but can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Firewall Management

- Configuration of address translation (NAT/PAT)
- Configuration of firewall rule management
- Virtualization cluster configuration support (if needed)
- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of Cisco AnyConnect including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing Cisco client software
    - Site-to-site VPN management
        - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
        - Troubleshooting / support of VPN tunnel establishment

Patching and Upgrades

- Periodic reviews of critical patches

- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the ASAv50 software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

End of Support

The Cisco ASAv50 is subject to an EOS Date, as described above in this SOW.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Intellectual Property in and to the Services belonging to Cisco or other Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide virtualizing resources to meet or exceed the Managed ASAv50 HA Infrastructure specifications.
    - Combined minimum virtualized resources necessary to run the Managed ASAv50 HA are as follows:
        - 16 vCPU
        - 32 GB memory *
        - 16 GB storage

  * Up to 16 GB of memory is required to support 50 Cisco AnyConnect User Sessions

- Provide and configure desired internal and external network services
- Open any necessary ports and conduits between the Appliance and Company s management services
- Client is responsible for performing all Security Operations Center (SOC) services including but not limited to:
    - Security incident response
    - Security incident identification, analysis, defense, investigation and reporting
    - Data breach investigation and reporting
    - Security gap analysis

Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco ASAv50 software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf and the Cisco Secure Supplemental End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/anyconnect-SEULA-v4x.pdf (collectively the Cisco Terms).

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at OneNeck or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Intellectual Property rights including pursuing an action against any breaching third parties.

602362 ASAv5 VPN Connectivity Licenses For 25 User Sessions

Company's Responsibilities and Included Features

For each quantity of this ItemID subscribed to, Company will provide 25 Cisco AnyConnect Plus Licenses.

Note: The total number of Cisco AnyConnect Plus Licenses cannot exceed 50.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Current subscription for Company s Managed Cisco Adaptive Security Virtual Appliance (ASAv5).

Additional ASAv resources for CPU memory and storage may be required depending on number of additional VPN Connectivity Licenses used.

End User License Agreement

Client agrees that the Cisco ASAv5 software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf

602364 Managed Cisco Adaptive Security Virtual Appliance (ASAv5)

The Managed Cisco Adaptive Security Virtual Appliance Model 5 (Managed ASAv5) service is a combination of Company managed services for a firewall and Cisco software licensing for the purpose of running a single (non-redundant) ASAv5 firewall on virtualized infrastructure provided by Client or contracted to be provided by Company.

Definitions

Intellectual Property: any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Feature Specification

The following table provides the ASAv5 feature specifications that Company will manage:

Feature	Entitlement / Managed Support	Licensing Included
Stateful inspection firewall throughput (maximum) *	100 Mbps	Yes
Stateful inspection firewall throughput (multiprotocol) **	50 Mbps	Yes
Advanced Encryption Standard (AES) VPN throughput***	30 Mbps	Yes
Connections per second	8,000	Yes
Concurrent sessions	50,000	Yes
VLANs	25	Yes
Bridge groups	12	Yes
IPsec VPN peers****	25	Yes
Cisco AnyConnect or clientless VPN user sessions*****	50	Yes

Note: Cisco s Cisco Adaptive Security Virtual Appliance v5 may include software features not listed in the table above. Any unlisted services are not within the scope of Company s managed support of virtual appliance.

*Maximum throughput measured by Cisco with User Datagram Protocol (UDP) traffic under ideal conditions.

** Multiprotocol refers to a traffic profile consisting primarily of TCP-based protocols or applications like HTTP, SMTP, FTP, IMAPv4, BitTorrent, and DNS.

*** The VPN throughput and the number of sessions depend on the ASA device configuration and VPN traffic patterns. These elements should be taken into consideration as part of your capacity planning.

**** Note, additional IPSec VPN peers (>25) are available and can be purchased from Company under a separate ItemID.

*****Cisco AnyConnect or clientless VPN user sessions are not included with this ItemID, but can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Firewall Management

- Configuration of address translation (NAT/PAT)
- Configuration of firewall rule management
- Virtualization cluster configuration support (if needed)
- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of Cisco AnyConnect including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing Cisco client software

Site-to-site VPN management

- Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
- Troubleshooting / support of VPN tunnel establishment

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the ASAv5 software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

End of Support

The Cisco ASAv5 is subject to an EOS Date, as described above in this SOW.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Intellectual Property in and to the Services belonging to Cisco or other Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide virtualizing resources to meet or exceed the Managed ASAv5 Infrastructure specifications.
    - Minimum virtualized resources necessary to run the Managed ASAv5 are as follows:
        - 1 vCPU
        - 2 GB memory *
        - 8 GB storage

  * Up to 8 GB of memory is required to support 50 Cisco AnyConnect User Sessions

- Provide and configure desired internal and external network services

- Open any necessary ports and conduits between the Appliance and Company s management services
- Specify and implement, desired fault tolerance. Note, the Managed ASAv5 is a single (1) virtual appliance and non-redundant. Should Client desire fault tolerance from a fail-over, reboot, or system maintenance window, a second (2 total) Managed ASAv5 should be deployed and configured for high-availability. That service is available from Company under a separate ItemID.
- Client is responsible for performing all Security Operations Center (SOC) services including but not limited to:
    - Security incident response
    - Security incident identification, analysis, defense, investigation and reporting
    - Data breach investigation and reporting
    - Security gap analysis
    - Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco ASAv5 software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf and the Cisco Secure Supplemental End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/anyconnect-SEULA-v4x.pdf (collectively the Cisco Terms).

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at OneNeck or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Intellectual Property rights including pursuing an action against any breaching third parties.

602365 Managed Cisco Adaptive Security Virtual Appliance (ASAv50)

The Managed Cisco Adaptive Security Virtual Appliance Model 50 (Managed ASAv50) service is a combination of Company managed services for a firewall and Cisco software licensing for the purpose of running a single (non-redundant) ASAv50 firewall on virtualized infrastructure provided by Client or contracted to be provided by Company.

Definitions

Intellectual Property: any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Feature Specification

The following table provides the ASAv50 feature specifications that Company will manage:

Feature	Entitlement / Managed Support	Licensing Included
Stateful inspection firewall throughput (maximum) *	10 Gbps	Yes
Stateful inspection firewall throughput (multiprotocol) **	5 Gbps	Yes
Advanced Encryption Standard (AES) VPN throughput***	4 Gbps	Yes
Connections per second	120,000	Yes

Concurrent sessions	2,000,000	Yes
VLANs	1,024	Yes
Bridge groups	250	Yes
IPsec VPN peers****	25	Yes
Cisco AnyConnect or clientless VPN user sessions*****	10,000	Yes

Note: Cisco s Cisco Adaptive Security Virtual Appliance v50 may include software features not listed in the table above. Any unlisted services are not within the scope of Company s managed support of virtual appliance.

*Maximum throughput measured by Cisco with User Datagram Protocol (UDP) traffic under ideal conditions.

** Multiprotocol refers to a traffic profile consisting primarily of TCP-based protocols or applications like HTTP, SMTP, FTP, IMAPv4, BitTorrent, and DNS.

*** The VPN throughput and the number of sessions depend on the ASA device configuration and VPN traffic patterns. These elements should be taken into consideration as part of your capacity planning.

**** Note, additional IPSec VPN peers (>25) are available and can be purchased from Company under a separate ItemID.

*****Cisco AnyConnect or clientless VPN user sessions are not included with this ItemID, but can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Firewall Management

- Configuration of address translation (NAT/PAT)
- Configuration of firewall rule management
- Virtualization cluster configuration support (if needed)
- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of Cisco AnyConnect including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing Cisco client software
    - Site-to-site VPN management
        - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
        - Troubleshooting / support of VPN tunnel establishment

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the ASAv5 software (including major upgrades) will be conducted at Company s discretion and in

accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

End of Support

The Cisco ASAv50 is subject to an EOS Date, as described above in this SOW.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Intellectual Property in and to the Services belonging to Cisco or other Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide virtualizing resources to meet or exceed the Managed ASAv50 Infrastructure specifications.
    - Minimum virtualized resources necessary to run the Managed ASAv50 are as follows:
        - 8 vCPU
        - 16 GB memory *
        - 8 GB storage

* Up to 8 GB of memory is required to support 50 Cisco AnyConnect User Sessions

- Provide and configure desired internal and external network services
- Open any necessary ports and conduits between the Appliance and Company s management services
- Specify and implement, desired fault tolerance. Note, the Managed ASAv50 is a single (1) virtual appliance and non-redundant. Should Client desire fault tolerance from a fail-over, reboot, or system maintenance window, a second (2 total) Managed ASAv50 should be deployed and configured for high-availability. That service is available from Company under a separate ItemID.
- Client is responsible for performing all Security Operations Center (SOC) services including but not limited to:
    - Security incident response
    - Security incident identification, analysis, defense, investigation and reporting
    - Data breach investigation and reporting
    - Security gap analysis

Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco ASAv50 software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf and the Cisco Secure Supplemental End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/anyconnect-SEULA-v4x.pdf (collectively the Cisco Terms).

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at OneNeck or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Intellectual Property rights including pursuing an action against any breaching third parties.

602366 Managed Cisco Adaptive Security Virtual Appliance (ASAv10) HA Pair

The Managed Cisco Adaptive Security Virtual Appliance ASAv10 HA (Managed ASAv10 HA) service is a combination of Company managed services for a pair of ASAv10s deployed in a high availability configuration (active/standby) and Cisco software licensing for the purpose of running a Managed ASAv10 HA firewall on virtualized infrastructure provided by Client or contracted to be provided by Company.

Definitions

Intellectual Property: any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Feature Specification

The following table provides the ASAv10 feature specifications that Company will manage:

Feature	**Entitlement / Managed Support**	**Licensing Included**
Stateful inspection firewall throughput (maximum) *	1 Gbps	Yes
Stateful inspection firewall throughput (multiprotocol) **	500 Mbps	Yes
Advanced Encryption Standard (AES) VPN throughput***	750 Mbps	Yes
Connections per second	20,000	Yes
Concurrent sessions	100,000	Yes
VLANs	50	Yes
Bridge groups	25	Yes
IPsec VPN peers****	25	Yes
Cisco AnyConnect or clientless VPN user sessions*****	250	Yes

Note: Cisco s Cisco Adaptive Security Virtual Appliance v10 may include software features not listed in the table above. Any unlisted services are not within the scope of Company s managed support of virtual appliance.

*Maximum throughput measured by Cisco with User Datagram Protocol (UDP) traffic under ideal conditions.

** Multiprotocol refers to a traffic profile consisting primarily of TCP-based protocols or applications like HTTP, SMTP, FTP, IMAPv4, BitTorrent, and DNS.

*** The VPN throughput and the number of sessions depend on the ASA device configuration and VPN traffic patterns. These elements should be taken into consideration as part of your capacity planning.

**** Note, additional IPSec VPN peers (>25) are available and can be purchased from Company under a separate ItemID.

*****Cisco AnyConnect or clientless VPN user sessions are not included with this ItemID, but can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Firewall Management

- Configuration of address translation (NAT/PAT)
- Configuration of firewall rule management
- Virtualization cluster configuration support (if needed)
- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of Cisco AnyConnect including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing Cisco client software
    - Site-to-site VPN management
        - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
        - Troubleshooting / support of VPN tunnel establishment

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the ASAv10 software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

End of Support

The Cisco ASAv10 is subject to an EOS Date, as described above in this SOW.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Intellectual Property in and to the Services belonging to Cisco or other Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide virtualizing resources to meet or exceed the Managed ASAv10 HA Infrastructure specifications.
    - Combined minimum virtualized resources necessary to run the Managed ASAv10 HA are as follows:
        - 4 vCPU
        - 8 GB memory *
        - 16 GB storage

* Up to 16 GB of memory is required to support 50 Cisco AnyConnect User Sessions

- Provide and configure desired internal and external network services
- Open any necessary ports and conduits between the Appliance and Company s management services
- Client is responsible for performing all Security Operations Center (SOC) services including but not limited to:
    - Security incident response
    - Security incident identification, analysis, defense, investigation and reporting
    - Data breach investigation and reporting
    - Security gap analysis
    - Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco ASAv10 software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf and the Cisco Secure Supplemental End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/anyconnect-SEULA-v4x.pdf (collectively the Cisco Terms).

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and

further agrees that it will, at OneNeck or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Intellectual Property rights including pursuing an action against any breaching third parties.

602367 ASAv10 VPN Connectivity Licenses For 25 User Sessions

Company's Responsibilities and Included Features

For each quantity of this ItemID subscribed to, Company will provide 25 Cisco AnyConnect Plus Licenses.

Note: The total number of Cisco AnyConnect Plus Licenses cannot exceed 250.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Current subscription for Company s Managed Cisco Adaptive Security Virtual Appliance (ASAv10).

Additional ASAv resources for CPU memory and storage may be required depending on number of additional VPN Connectivity Licenses used.

End User License Agreement

Client agrees that the Cisco ASAv10 software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf

602368 GoDaddy Deluxe SSL OV 1 year - Protect All Subdomains (Wildcard) with Support

This ItemID contains an order for Secure Socket Layer (SSL) certificates provided by GoDaddy.com, LLC. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the GoDaddy offerings will be provided and made by GoDaddy.com, LLC. and may be subject to change as determined by GoDaddy.com, LLC.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by GoDaddy.

Client agrees that the GoDaddy Offerings are subject to the GoDaddy Certificate Services Agreement available at https://www.godaddy.com/legal/agreements/certificate-services-agreement, which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide an annual subscription-based GoDaddy Deluxe SSL Organization Validation (OV) Certificate to protect all subdomains (Wildcard) including:

- Installation of SSL certificate on Company managed servers/devices/applications
- Notification of upcoming renewal, at least 45 days in advance of the renewal
- Automatic annual renewal of the certificate
- Troubleshooting of SSL certificate errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of cancellation of subscription at least 30 days in advance of the automatic annual renewal; subscription will otherwise automatically renew
- Provide Company with a list of servers/devices/applications where the certificate is used
- Notify Company of any changes to the servers/devices/applications where the certificate is used
- Installation of the SSL certificate on any non-managed servers/device/application

602388 NGFWv VPN Connectivity Licenses for 25 User Sessions

Company's Responsibilities and Included Features

For each quantity of this ItemID subscribed to, Company will provide 25 Cisco AnyConnect Plus Licenses.

Note: The total number of Cisco AnyConnect Plus Licenses cannot exceed 250 for 4 vCPU or 8 vCPU. The total number of Cisco AnyConnect Plus Licenses cannot exceed 750 for 12 vCPU.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Current subscription for Company s Managed Cisco Firepower Next-Generation Firewall Virtual Appliance (NGFWv).

Additional NGFWv resources for CPU memory and storage may be required depending on number of additional VPN Connectivity Licenses used.

End User License Agreement

Client agrees that the Cisco NGFWv software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf

602397 GoDaddy Standard SSL DV 1 year - Protect 1 Website with Support

This ItemID contains an order for Secure Socket Layer (SSL) certificates provided by GoDaddy.com, LLC. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the GoDaddy offerings will be provided and made by GoDaddy.com, LLC. and may be subject to change as determined by GoDaddy.com, LLC.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by GoDaddy.

Client agrees that the GoDaddy Offerings are subject to the GoDaddy Certificate Services Agreement available at https://www.godaddy.com/legal/agreements/certificate-services-agreement, which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide an annual subscription-based GoDaddy Standard SSL Domain Validation (DV) Certificate to protect 1 website including:

- Installation of SSL certificate on Company managed servers/devices/applications
- Notification of upcoming renewal, at least 45 days in advance of the renewal
- Automatic annual renewal of the certificate
- Troubleshooting of SSL certificate errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of cancellation of subscription at least 30 days in advance of the automatic annual renewal; subscription will otherwise automatically renew
- Provide Company with a list of servers/devices/applications where the certificate is used
- Notify Company of any changes to the servers/devices/applications where the certificate is used
- Installation of the SSL certificate on any non-managed servers/device/application

602398 GoDaddy Standard SSL DV 1 year - Protect All Subdomains (Wildcard) with Support

This ItemID contains an order for Secure Socket Layer (SSL) certificates provided by GoDaddy.com, LLC. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the GoDaddy offerings will be provided and made by GoDaddy.com, LLC. and may be subject to change as determined by GoDaddy.com, LLC.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by GoDaddy.

Client agrees that the GoDaddy Offerings are subject to the GoDaddy Certificate Services Agreement available at

https://www.godaddy.com/legal/agreements/certificate-services-agreement, which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide an annual subscription-based GoDaddy Standard SSL Domain Validation (DV) Certificate to protect all subdomains (wildcard) including:

- Installation of SSL certificate on Company managed servers/devices/applications
- Notification of upcoming renewal, at least 45 days in advance of the renewal
- Automatic annual renewal of the certificate
- Troubleshooting of SSL certificate errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of cancellation of subscription at least 30 days in advance of the automatic annual renewal; subscription will otherwise automatically renew
- Provide Company with a list of servers/devices/applications where the certificate is used
- Notify Company of any changes to the servers/devices/applications where the certificate is used
- Installation of the SSL certificate on any non-managed servers/device/application

602399 GoDaddy Standard SSL DV 1 year - Protect Multiple Websites (UCC/SAN) Up to 5 Sites with Support

This ItemID contains an order for Secure Socket Layer (SSL) certificates provided by GoDaddy.com, LLC. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the GoDaddy offerings will be provided and made by GoDaddy.com, LLC. and may be subject to change as determined by GoDaddy.com, LLC.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by GoDaddy.

Client agrees that the GoDaddy Offerings are subject to the GoDaddy Certificate Services Agreement available at https://www.godaddy.com/legal/agreements/certificate-services-agreement, which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide an annual subscription-based GoDaddy Standard SSL Domain Validation (DV) Certificate to protect multiple websites (UCC/SAN) up to 5 sites including:

- Installation of SSL certificate on Company managed servers/devices/applications
- Notification of upcoming renewal, at least 45 days in advance of the renewal
- Automatic annual renewal of the certificate
- Troubleshooting of SSL certificate errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of cancellation of subscription at least 30 days in advance of the automatic annual renewal; subscription will otherwise automatically renew
- Provide Company with a list of servers/devices/applications where the certificate is used
- Notify Company of any changes to the servers/devices/applications where the certificate is used
- Installation of the SSL certificate on any non-managed servers/device/application

602400 GoDaddy Standard SSL DV 1 year - Up to 10 Sites with Support

This ItemID contains an order for Secure Socket Layer (SSL) certificates provided by GoDaddy.com, LLC. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the GoDaddy offerings will be provided and made by GoDaddy.com, LLC. and may be subject to change as determined by GoDaddy.com, LLC.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by GoDaddy.

Client agrees that the GoDaddy Offerings are subject to the GoDaddy Certificate Services Agreement available at https://www.godaddy.com/legal/agreements/certificate-services-agreement, which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide an annual subscription-based GoDaddy Standard SSL Domain Validation (DV) Certificate to protect multiple websites (UCC/SAN) up to 10 sites including:

- Installation of SSL certificate on Company managed servers/devices/applications
- Notification of upcoming renewal, at least 45 days in advance of the renewal
- Automatic annual renewal of the certificate
- Troubleshooting of SSL certificate errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of cancellation of subscription at least 30 days in advance of the automatic annual renewal; subscription will otherwise automatically renew
- Provide Company with a list of servers/devices/applications where the certificate is used
- Notify Company of any changes to the servers/devices/applications where the certificate is used
- Installation of the SSL certificate on any non-managed servers/device/application

602401 GoDaddy Standard SSL DV 1 year - Up to 15 Sites with Support

This ItemID contains an order for Secure Socket Layer (SSL) certificates provided by GoDaddy.com, LLC. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the GoDaddy offerings will be provided and made by GoDaddy.com, LLC. and may be subject to change as determined by GoDaddy.com, LLC.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by GoDaddy.

Client agrees that the GoDaddy Offerings are subject to the GoDaddy Certificate Services Agreement available at https://www.godaddy.com/legal/agreements/certificate-services-agreement, which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide an annual subscription-based GoDaddy Standard SSL Domain Validation (DV) Certificate to protect multiple websites (UCC/SAN) up to 15 sites including:

- Installation of SSL certificate on Company managed servers/devices/applications
- Notification of upcoming renewal, at least 45 days in advance of the renewal
- Automatic annual renewal of the certificate
- Troubleshooting of SSL certificate errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of cancellation of subscription at least 30 days in advance of the automatic annual renewal; subscription will otherwise automatically renew
- Provide Company with a list of servers/devices/applications where the certificate is used
- Notify Company of any changes to the servers/devices/applications where the certificate is used
- Installation of the SSL certificate on any non-managed servers/device/application

602402 GoDaddy Deluxe SSL OV 1 year - Protect 1 Website with Support

This ItemID contains an order for Secure Socket Layer (SSL) certificates provided by GoDaddy.com, LLC. Client agrees,

acknowledges, and understands that the actual manufacture, provision, and performance of the GoDaddy offerings will be provided and made by GoDaddy.com, LLC. and may be subject to change as determined by GoDaddy.com, LLC.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by GoDaddy.

Client agrees that the GoDaddy Offerings are subject to the GoDaddy Certificate Services Agreement available at https://www.godaddy.com/legal/agreements/certificate-services-agreement, which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide an annual subscription-based GoDaddy Deluxe SSL Organization Validation (OV) Certificate to protect 1 website including:

- Installation of SSL certificate on Company managed servers/devices/applications
- Notification of upcoming renewal, at least 45 days in advance of the renewal
- Automatic annual renewal of the certificate
- Troubleshooting of SSL certificate errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of cancellation of subscription at least 30 days in advance of the automatic annual renewal; subscription will otherwise automatically renew
- Provide Company with a list of servers/devices/applications where the certificate is used
- Notify Company of any changes to the servers/devices/applications where the certificate is used
- Installation of the SSL certificate on any non-managed servers/device/application

602403 GoDaddy Deluxe SSL OV 1 year - Protect Multiple Websites (UCC/SAN) Up to 5 Sites with Support

This ItemID contains an order for Secure Socket Layer (SSL) certificates provided by GoDaddy.com, LLC. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the GoDaddy offerings will be provided and made by GoDaddy.com, LLC. and may be subject to change as determined by GoDaddy.com, LLC.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by GoDaddy.

Client agrees that the GoDaddy Offerings are subject to the GoDaddy Certificate Services Agreement available at https://www.godaddy.com/legal/agreements/certificate-services-agreement, which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide an annual subscription-based GoDaddy Deluxe SSL Organization Validation (OV) Certificate to protect multiple websites (UCC/SAN) up to 5 sites including:

- Installation of SSL certificate on Company managed servers/devices/applications
- Notification of upcoming renewal, at least 45 days in advance of the renewal
- Automatic annual renewal of the certificate
- Troubleshooting of SSL certificate errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of cancellation of subscription at least 30 days in advance of the automatic annual renewal; subscription will otherwise automatically renew
- Provide Company with a list of servers/devices/applications where the certificate is used
- Notify Company of any changes to the servers/devices/applications where the certificate is used
- Installation of the SSL certificate on any non-managed servers/device/application

602404 GoDaddy Deluxe SSL OV 1 year - Protect Multiple Websites (UCC/SAN) Up to 10 Sites with Support

This ItemID contains an order for Secure Socket Layer (SSL) certificates provided by GoDaddy.com, LLC. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the GoDaddy offerings will be provided and made by GoDaddy.com, LLC. and may be subject to change as determined by GoDaddy.com, LLC.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by GoDaddy.

Client agrees that the GoDaddy Offerings are subject to the GoDaddy Certificate Services Agreement available at https://www.godaddy.com/legal/agreements/certificate-services-agreement, which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide an annual subscription-based GoDaddy Deluxe SSL Organization Validation (OV) Certificate to protect multiple websites (UCC/SAN) up to 10 sites including:

- Installation of SSL certificate on Company managed servers/devices/applications
- Notification of upcoming renewal, at least 45 days in advance of the renewal
- Automatic annual renewal of the certificate
- Troubleshooting of SSL certificate errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of cancellation of subscription at least 30 days in advance of the automatic annual renewal; subscription will otherwise automatically renew
- Provide Company with a list of servers/devices/applications where the certificate is used
- Notify Company of any changes to the servers/devices/applications where the certificate is used
- Installation of the SSL certificate on any non-managed servers/device/application

602405 GoDaddy Deluxe SSL OV 1 year - Protect Multiple Websites (UCC/SAN) Up to 15 Sites with Support

This ItemID contains an order for Secure Socket Layer (SSL) certificates provided by GoDaddy.com, LLC. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the GoDaddy offerings will be provided and made by GoDaddy.com, LLC. and may be subject to change as determined by GoDaddy.com, LLC.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by GoDaddy.

Client agrees that the GoDaddy Offerings are subject to the GoDaddy Certificate Services Agreement available at https://www.godaddy.com/legal/agreements/certificate-services-agreement, which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide an annual subscription-based GoDaddy Deluxe SSL Organization Validation (OV) Certificate to protect multiple websites (UCC/SAN) up to 15 sites including:

- Installation of SSL certificate on Company managed servers/devices/applications
- Notification of upcoming renewal, at least 45 days in advance of the renewal
- Automatic annual renewal of the certificate
- Troubleshooting of SSL certificate errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of cancellation of subscription at least 30 days in advance of the automatic annual renewal; subscription will otherwise automatically renew
- Provide Company with a list of servers/devices/applications where the certificate is used

- Notify Company of any changes to the servers/devices/applications where the certificate is used
- Installation of the SSL certificate on any non-managed servers/device/application

602406 GoDaddy Premium SSL EV 1 year - Protect 1 Website with Support

This ItemID contains an order for Secure Socket Layer (SSL) certificates provided by GoDaddy.com, LLC. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the GoDaddy offerings will be provided and made by GoDaddy.com, LLC. and may be subject to change as determined by GoDaddy.com, LLC.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by GoDaddy.

Client agrees that the GoDaddy Offerings are subject to the GoDaddy Certificate Services Agreement available at https://www.godaddy.com/legal/agreements/certificate-services-agreement, which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide an annual subscription-based GoDaddy Premium SSL Extended Validation (EV) Certificate to protect 1 website including:

- Installation of SSL certificate on Company managed servers/devices/applications
- Notification of upcoming renewal, at least 45 days in advance of the renewal
- Automatic annual renewal of the certificate
- Troubleshooting of SSL certificate errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of cancellation of subscription at least 30 days in advance of the automatic annual renewal; subscription will otherwise automatically renew
- Provide Company with a list of servers/devices/applications where the certificate is used
- Notify Company of any changes to the servers/devices/applications where the certificate is used
- Installation of the SSL certificate on any non-managed servers/device/application

602407 GoDaddy Premium SSL EV 1 year - Protect Multiple Websites (UCC/SAN) Up to 5 Sites with Support

This ItemID contains an order for Secure Socket Layer (SSL) certificates provided by GoDaddy.com, LLC. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the GoDaddy offerings will be provided and made by GoDaddy.com, LLC. and may be subject to change as determined by GoDaddy.com, LLC.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by GoDaddy.

Client agrees that the GoDaddy Offerings are subject to the GoDaddy Certificate Services Agreement available at https://www.godaddy.com/legal/agreements/certificate-services-agreement, which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide an annual subscription-based GoDaddy Premium SSL Extended Validation (EV) Certificate to protect multiple websites (UCC/SAN) up to 5 sites including:

- Installation of SSL certificate on Company managed servers/devices/applications
- Notification of upcoming renewal, at least 45 days in advance of the renewal
- Automatic annual renewal of the certificate
- Troubleshooting of SSL certificate errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of cancellation of subscription at least 30 days in advance of the automatic annual renewal; subscription will otherwise automatically renew
- Provide Company with a list of servers/devices/applications where the certificate is used
- Notify Company of any changes to the servers/devices/applications where the certificate is used
- Installation of the SSL certificate on any non-managed servers/device/application

602408 GoDaddy Premium SSL EV 1 year - Protect Multiple Websites (UCC/SAN) Up to 10 Sites with Support

This ItemID contains an order for Secure Socket Layer (SSL) certificates provided by GoDaddy.com, LLC. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the GoDaddy offerings will be provided and made by GoDaddy.com, LLC. and may be subject to change as determined by GoDaddy.com, LLC.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by GoDaddy.

Client agrees that the GoDaddy Offerings are subject to the GoDaddy Certificate Services Agreement available at https://www.godaddy.com/legal/agreements/certificate-services-agreement, which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide an annual subscription-based GoDaddy Premium SSL Extended Validation (EV) Certificate to protect multiple websites (UCC/SAN) up to 10 sites including:

- Installation of SSL certificate on Company managed servers/devices/applications
- Notification of upcoming renewal, at least 45 days in advance of the renewal
- Automatic annual renewal of the certificate
- Troubleshooting of SSL certificate errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of cancellation of subscription at least 30 days in advance of the automatic annual renewal; subscription will otherwise automatically renew
- Provide Company with a list of servers/devices/applications where the certificate is used
- Notify Company of any changes to the servers/devices/applications where the certificate is used
- Installation of the SSL certificate on any non-managed servers/device/application

602409 GoDaddy Premium SSL EV 1 year - Protect Multiple Websites (UCC/SAN) Up to 15 Sites with Support

This ItemID contains an order for Secure Socket Layer (SSL) certificates provided by GoDaddy.com, LLC. Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the GoDaddy offerings will be provided and made by GoDaddy.com, LLC. and may be subject to change as determined by GoDaddy.com, LLC.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by GoDaddy.

Client agrees that the GoDaddy Offerings are subject to the GoDaddy Certificate Services Agreement available at https://www.godaddy.com/legal/agreements/certificate-services-agreement, which are hereby incorporated into this Statement of Work.

Company's Responsibilities and Included Features

Company will provide an annual subscription-based GoDaddy Premium SSL Extended Validation (EV) Certificate to protect multiple websites (UCC/SAN) up to 15 sites including:

- Installation of SSL certificate on Company managed servers/devices/applications
- Notification of upcoming renewal, at least 45 days in advance of the renewal
- Automatic annual renewal of the certificate
- Troubleshooting of SSL certificate errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of cancellation of subscription at least 30 days in advance of the automatic annual renewal; subscription will otherwise automatically renew
- Provide Company with a list of servers/devices/applications where the certificate is used
- Notify Company of any changes to the servers/devices/applications where the certificate is used
- Installation of the SSL certificate on any non-managed servers/device/application

602744 Cisco NGFWv Base + Threat + AMP (1G) Licenses

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Base + Threat + AMP 1G (NGFWv Base + Threat + AMP 1G) offers threat protection features and centralized management as follows:

- Base NGFWv includes Application Visibility and Control (AVC) to reduce the potential surface area of attacks through granular control of thousands of applications and enforcement of mobile, social and other acceptable use policies
- Threat subscription includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control and Security Intelligence filtering
- Advanced Malware Protection (AMP) for Networks subscription enables detection, blocking, tracking, analysis and containment of targeted and persistent malware

1G (G = gigabits per second) is the theoretical maximum throughput, however, short-term limited bursts greater than 1G in throughput are allowed by the system. If throughput exceeds 1G, additional charges may apply

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Performance Specifications for NGFWv (ESXi/KVM)

Specification	**4 vCPU**	**8 vCPU**	**12 vCPU**
Throughput: FW + AVC (1024B)	3 Gbps	5.5 Gbps	10 Gbps
Throughput: FW + AVC + IPS (1024B)	3 Gbps	5.5 Gbps	10 Gbps
Throughput: FW + AVC (450B)	1.5 Gbps	3 Gbps	5 Gbps
Throughput: FW + AVC + IPS (450B)	1 Gbps	2 Gbps	3 Gbps
Maximum concurrent sessions	100,000	250,000	500,000
Maximum new connections per second	20,000	20,000	40,000
Maximum VPN peers*	250	250	750
IP Sec VPN throughput (1024B TCP w/Fastpath)	1.1 Gbps	2 Gbps	4 Gbps

*VPN peers are not included with this ItemID, but are available in the quantities noted above and can be purchased from Company under a separate ItemID.

Note: Above Performance Specifications should be considered general guidelines. Performance will vary depending on CPU type, CPU speed, cache, number of interfaces, features activated, network traffic protocol mix, packet size characteristics, etc . Performance is subject to change with new software releases.

System Requirements for NGFWv

Specification	**Description**
VMware and KVM: Virtual CPUs and memory (6.4 and above)	4 vCPU/8GB 8 vCPU/16GB

	12 vCPU/24GB
VMware and KVM: Virtual CPUs and memory (6.3 and above)	4 vCPU/8GB
Storage	50GB for all FTDv configurations
Hypervisor support	ESXi 6.0, 6.5, 6.7: KVM

Company's Responsibilities and Included Features

Licenses

Provide Cisco NGFWv Base + Threat + AMP 1G Licenses up to the quantity as stated in the Pricing Details above. Licenses will be provided on a monthly subscription basis.

Support Services for AMP

Upon Client request, escalate appropriate issues to Cisco TAC (Technical Assistance Center). Support services for Base + Threat are not included under this ItemID, but may be contracted under a separate ItemID.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless contracted separately with Company under this or another Executed Order, Client is responsible for the following:

Identification of moves/adds/changes and deletions to be performed by Company relating to Base + Threat.

Except as provided above, all support services for AMP.

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco NGFWv Base + Threat + AMP software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco

Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603283 Cisco Firepower NGFW Virtual - Base (1 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Base (1 Gbps) - Licenses and HA Management service is a combination of Company managed services for a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby) and Cisco software licensing for a pair of Cisco Firepower NGFW Virtual - Base (1 Gbps) for the purpose of running a managed Cisco Firepower NGFW Virtual, HA firewall with Base on virtualized infrastructure provided by Client or contracted to be provided by Company.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv)

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Base NGFWv includes Application Visibility and Control (AVC) to reduce the potential surface area of attacks through granular control of thousands of applications and enforces mobile, social, and other acceptable use policies

Performance Specifications for NGFWv

Refer to https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw-virtual/threat-defense-virtual-ngfwv-ds.html

VPN peers are not included with this ItemID, but are available and can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Firewall Management

- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
  - Local Database
  - Lightweight Directory Access Portal (LDAP)
  - Authentication, Authorization and Accounting (AAA)
  - Active Directory (AD)
  - Multifactor authentication (MFA)
  - Security Information and event Management (SIEM)
- Remote access VPN management
  - Deployment and support of remote access VPN management vendor software including:
    - Group policy definitions
    - External user database authentication integration
    - Certificate management
    - Client VPN access utilizing Cisco client software
  - Site-to-site VPN management
    - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
    - Troubleshooting / support of VPN tunnel establishment
- Vendor-provided NGFW policy updates (application control)
- Schedule standard reports (make recipient modifications if necessary)
- Vendor firewall management software

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Base

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Base
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Base
- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation, and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

Virtualization Platform

Provide a virtualization platform to host the virtual Cisco Firepower NGFW and the firewall management system

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide console access to the OS
- Provide Internet connection for usage metering purposes

End User License Agreement

Client agrees that the Cisco NGFWv Base software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603297 Cisco Firepower NGFW Virtual - Threat + URL (1 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + URL (1 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (1 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + URL (1 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (1 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + URL

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat + URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals,

extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + URL.

End User License Agreement

Client agrees that the Cisco NGFWv Threat + URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603358 Cisco Firepower NGFW Virtual - Threat (1 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat (1 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (1 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat (1 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (1 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a

time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat .

End User License Agreement

Client agrees that the Cisco NGFWv Threat software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603528 Cisco Firepower NGFW Virtual - Threat + Malware + URL (1 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + Malware Defense + URL (1 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (1 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + Malware Defense + URL (1 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + Malware Defense + URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (1 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies
- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + Malware Defense + URL

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat + URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + Malware Defense + URL.

End User License Agreement

Client agrees that the Cisco NGFWv Threat + Malware Defense + URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603529 Cisco Firepower NGFW Virtual - Base (5 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Base (5 Gbps) - Licenses and HA Management service is a combination of Company managed services for a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby) and Cisco

software licensing for a pair of Cisco Firepower NGFW Virtual - Base (5 Gbps) for the purpose of running a managed Cisco Firepower NGFW Virtual, HA firewall with Base on virtualized infrastructure provided by Client or contracted to be provided by Company.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv)

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Base NGFWv includes Application Visibility and Control (AVC) to reduce the potential surface area of attacks through granular control of thousands of applications and enforces mobile, social, and other acceptable use policies

Performance Specifications for NGFWv

Refer to https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw-virtual/threat-defense-virtual-ngfwv-ds.html

VPN peers are not included with this ItemID, but are available and can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Firewall Management

- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
  - Local Database
  - Lightweight Directory Access Portal (LDAP)
  - Authentication, Authorization and Accounting (AAA)
  - Active Directory (AD)
  - Multifactor authentication (MFA)
  - Security Information and event Management (SIEM)
- Remote access VPN management
  - Deployment and support of remote access VPN management vendor software including:
    - Group policy definitions
    - External user database authentication integration
    - Certificate management
    - Client VPN access utilizing Cisco client software
  - Site-to-site VPN management
    - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
    - Troubleshooting / support of VPN tunnel establishment
- Vendor-provided NGFW policy updates (application control)
- Schedule standard reports (make recipient modifications if necessary)
- Vendor firewall management software

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against

Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Base

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Base
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Base
- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation, and reporting
- Data breach investigation and reporting

- Security gap analysis
- Threat intelligence collection and analysis

Virtualization Platform

Provide a virtualization platform to host the virtual Cisco Firepower NGFW and the firewall management system

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide console access to the OS
- Provide Internet connection for usage metering purposes

End User License Agreement

Client agrees that the Cisco NGFWv Base software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603530 Cisco Firepower NGFW Virtual - Threat (5 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat (5 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (5 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat (5 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (5 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against

Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat .

End User License Agreement

Client agrees that the Cisco NGFWv Threat software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603599 Cisco Firepower NGFW Virtual - Malware (1 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Malware Defense (1 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (1 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Malware Defense (1 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Malware Defense running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (1 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Malware Defense

The following NGFW Support Services will be performed upon Client request:

- Client-identified moves/adds/changes and deletions relating to Malware
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Malware Defense .

End User License Agreement

Client agrees that the Cisco NGFWv Malware Defense software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603600 Cisco Firepower NGFW Virtual - Malware (100 Mbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Malware Defense (100 Mbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (100 Mbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Malware Defense (100 Mbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Malware Defense running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower

NGFW Virtual - Base (100 Mbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Malware Defense

The following NGFW Support Services will be performed upon Client request:

- Client-identified moves/adds/changes and deletions relating to Malware
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company

and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Malware Defense .

End User License Agreement

Client agrees that the Cisco NGFWv Malware Defense software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603601 Cisco Firepower NGFW Virtual - Malware (3 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Malware Defense (3 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (3 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Malware Defense (3 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Malware Defense running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (3 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis

Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Malware Defense

The following NGFW Support Services will be performed upon Client request:

- Client-identified moves/adds/changes and deletions relating to Malware
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Malware Defense .

End User License Agreement

Client agrees that the Cisco NGFWv Malware Defense software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603602 Cisco Firepower NGFW Virtual - Malware (5 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Malware Defense (5 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (5 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Malware Defense (5 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Malware Defense running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (5 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Malware Defense

The following NGFW Support Services will be performed upon Client request:

- Client-identified moves/adds/changes and deletions relating to Malware

- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Malware Defense .

End User License Agreement

Client agrees that the Cisco NGFWv Malware Defense software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603603 Cisco Firepower NGFW Virtual - Malware (10 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Malware Defense (10 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (10 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Malware Defense (10 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Malware Defense running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (10 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Malware Defense

The following NGFW Support Services will be performed upon Client request:

- Client-identified moves/adds/changes and deletions relating to Malware
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client

staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Malware Defense .

End User License Agreement

Client agrees that the Cisco NGFWv Malware Defense software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603604 Cisco Firepower NGFW Virtual - Malware (16 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Malware Defense (16 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (16 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Malware Defense (16 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Malware Defense running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (16 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Malware Defense

The following NGFW Support Services will be performed upon Client request:

- Client-identified moves/adds/changes and deletions relating to Malware
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Malware Defense .

End User License Agreement

Client agrees that the Cisco NGFWv Malware Defense software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603605 Cisco Firepower NGFW Virtual - Base (100 Mbs) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Base (100 Mbps) - Licenses and HA Management service is a combination of Company managed services for a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby) and Cisco software licensing for a pair of Cisco Firepower NGFW Virtual - Base (100 Mbps) for the purpose of running a managed Cisco Firepower NGFW Virtual, HA firewall with Base on virtualized infrastructure provided by Client or contracted to be provided by Company.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv)

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Base NGFWv includes Application Visibility and Control (AVC) to reduce the potential surface area of attacks through granular control of thousands of applications and enforces mobile, social, and other acceptable use policies

Performance Specifications for NGFWv

Refer to https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw-virtual/threat-defense-virtual-ngfwv-ds.html

VPN peers are not included with this ItemID, but are available and can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Firewall Management

- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
  - Local Database
  - Lightweight Directory Access Portal (LDAP)
  - Authentication, Authorization and Accounting (AAA)
  - Active Directory (AD)
  - Multifactor authentication (MFA)

Security Information and event Management (SIEM)

- Remote access VPN management
  - Deployment and support of remote access VPN management vendor software including:
    - Group policy definitions
    - External user database authentication integration
    - Certificate management
    - Client VPN access utilizing Cisco client software
  - Site-to-site VPN management
    - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
    - Troubleshooting / support of VPN tunnel establishment
- Vendor-provided NGFW policy updates (application control)
- Schedule standard reports (make recipient modifications if necessary)
- Vendor firewall management software

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Base

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Base
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Base
- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation, and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

Virtualization Platform

Provide a virtualization platform to host the virtual Cisco Firepower NGFW and the firewall management system

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide console access to the OS
- Provide Internet connection for usage metering purposes

End User License Agreement

Client agrees that the Cisco NGFWv Base software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603606 Cisco Firepower NGFW Virtual - Base (3 Gbs) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Base (3 Gbps) - Licenses and HA Management service is a combination of Company managed services for a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby) and Cisco software licensing for a pair of Cisco Firepower NGFW Virtual - Base (3 Gbps) for the purpose of running a managed Cisco Firepower NGFW Virtual, HA firewall with Base on virtualized infrastructure provided by Client or contracted to be provided by Company.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv)

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Base NGFWv includes Application Visibility and Control (AVC) to reduce the potential surface area of attacks through granular control of thousands of applications and enforces mobile, social, and other acceptable use policies

Performance Specifications for NGFWv

Refer to https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw-virtual/threat-defense-virtual-ngfwv-ds.html

VPN peers are not included with this ItemID, but are available and can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Firewall Management

- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
  - Local Database
  - Lightweight Directory Access Portal (LDAP)
  - Authentication, Authorization and Accounting (AAA)
  - Active Directory (AD)
  - Multifactor authentication (MFA)
  - Security Information and event Management (SIEM)
- Remote access VPN management
  - Deployment and support of remote access VPN management vendor software including:
    - Group policy definitions
    - External user database authentication integration
    - Certificate management
    - Client VPN access utilizing Cisco client software
  - Site-to-site VPN management
    - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
    - Troubleshooting / support of VPN tunnel establishment
- Vendor-provided NGFW policy updates (application control)
- Schedule standard reports (make recipient modifications if necessary)
- Vendor firewall management software

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a

time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Base

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Base
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Base
- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation, and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

Virtualization Platform

Provide a virtualization platform to host the virtual Cisco Firepower NGFW and the firewall management system

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide console access to the OS
- Provide Internet connection for usage metering purposes

End User License Agreement

Client agrees that the Cisco NGFWv Base software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603607 Cisco Firepower NGFW Virtual - Base (10 Gbs) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Base (10 Gbps) - Licenses and HA Management service is a combination of Company managed services for a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby) and Cisco software licensing for a pair of Cisco Firepower NGFW Virtual - Base (10 Gbps) for the purpose of running a managed Cisco Firepower NGFW Virtual, HA firewall with Base on virtualized infrastructure provided by Client or contracted to be provided by Company.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv)

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Base NGFWv includes Application Visibility and Control (AVC) to reduce the potential surface area of attacks through granular control of thousands of applications and enforces mobile, social, and other acceptable use policies

Performance Specifications for NGFWv

Refer to https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw-virtual/threat-defense-virtual-ngfwv-ds.html

VPN peers are not included with this ItemID, but are available and can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Firewall Management

- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
  - Local Database
  - Lightweight Directory Access Portal (LDAP)
  - Authentication, Authorization and Accounting (AAA)
  - Active Directory (AD)

        - Multifactor authentication (MFA)
        - Security Information and event Management (SIEM)
    - Remote access VPN management
        - Deployment and support of remote access VPN management vendor software including:
            - Group policy definitions
            - External user database authentication integration
            - Certificate management
            - Client VPN access utilizing Cisco client software
        - Site-to-site VPN management
            - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
            - Troubleshooting / support of VPN tunnel establishment
    - Vendor-provided NGFW policy updates (application control)
    - Schedule standard reports (make recipient modifications if necessary)
    - Vendor firewall management software

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Base

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Base
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Base
- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation, and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

Virtualization Platform

Provide a virtualization platform to host the virtual Cisco Firepower NGFW and the firewall management system

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide console access to the OS
- Provide Internet connection for usage metering purposes

End User License Agreement

Client agrees that the Cisco NGFWv Base software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603608 Cisco Firepower NGFW Virtual - Base (16 Gbs) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Base (16 Gbps) - Licenses and HA Management service is a combination of Company managed services for a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby) and Cisco software licensing for a pair of Cisco Firepower NGFW Virtual - Base (16 Gbps) for the purpose of running a managed Cisco

Firepower NGFW Virtual, HA firewall with Base on virtualized infrastructure provided by Client or contracted to be provided by Company.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv)

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Base NGFWv includes Application Visibility and Control (AVC) to reduce the potential surface area of attacks through granular control of thousands of applications and enforces mobile, social, and other acceptable use policies

Performance Specifications for NGFWv

Refer to https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw-virtual/threat-defense-virtual-ngfwv-ds.html

VPN peers are not included with this ItemID, but are available and can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Firewall Management

- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
  - Local Database
  - Lightweight Directory Access Portal (LDAP)
  - Authentication, Authorization and Accounting (AAA)
  - Active Directory (AD)
  - Multifactor authentication (MFA)
  - Security Information and event Management (SIEM)
- Remote access VPN management
  - Deployment and support of remote access VPN management vendor software including:
    - Group policy definitions
    - External user database authentication integration
    - Certificate management
    - Client VPN access utilizing Cisco client software
  - Site-to-site VPN management
    - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
    - Troubleshooting / support of VPN tunnel establishment
- Vendor-provided NGFW policy updates (application control)
- Schedule standard reports (make recipient modifications if necessary)
- Vendor firewall management software

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements

will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Base

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Base
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Base
- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation, and reporting
- Data breach investigation and reporting
- Security gap analysis

- Threat intelligence collection and analysis

Virtualization Platform

Provide a virtualization platform to host the virtual Cisco Firepower NGFW and the firewall management system

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide console access to the OS
- Provide Internet connection for usage metering purposes

End User License Agreement

Client agrees that the Cisco NGFWv Base software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603609 Cisco Firepower NGFW Virtual - Threat (100 Mbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat (100 Mbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (100 Mbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat (100 Mbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (100 Mbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements

will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat .

End User License Agreement

Client agrees that the Cisco NGFWv Threat software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco

Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603610 Cisco Firepower NGFW Virtual - Threat (3 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat (3 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (3 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat (3 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (3 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat .

End User License Agreement

Client agrees that the Cisco NGFWv Threat software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603611 Cisco Firepower NGFW Virtual - Threat (10 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat (10 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (10 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat (10 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (10

Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services

Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat .

End User License Agreement

Client agrees that the Cisco NGFWv Threat software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603612 Cisco Firepower NGFW Virtual - Threat (16 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat (16 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (16 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat (16 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (16 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches

Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat .

End User License Agreement

Client agrees that the Cisco NGFWv Threat software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603613 Cisco Firepower NGFW Virtual - Threat + URL (100 Mbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + URL (100 Mbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (100 Mbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + URL (100 Mbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (100 Mbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + URL

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat + URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + URL.

End User License Agreement

Client agrees that the Cisco NGFWv Threat + URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and

further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603614 Cisco Firepower NGFW Virtual - Threat + URL (3 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + URL (3 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (3 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + URL (3 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (3 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + URL

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat + URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + URL.

End User License Agreement

Client agrees that the Cisco NGFWv Threat + URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603615 Cisco Firepower NGFW Virtual - Threat + URL (5 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + URL (5 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (5 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + URL (5 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (5 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + URL

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat + URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company

and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + URL.

End User License Agreement

Client agrees that the Cisco NGFWv Threat + URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603616 Cisco Firepower NGFW Virtual - Threat + URL (10 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + URL (10 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (10 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + URL (10 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (10 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies

Company's Responsibilities and Included Features

Patching and Upgrades

Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + URL

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat + URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + URL.

End User License Agreement

Client agrees that the Cisco NGFWv Threat + URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603617 Cisco Firepower NGFW Virtual - Threat + URL (16 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + URL (16 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (16 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + URL (16 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (16 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + URL

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat + URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + URL.

End User License Agreement

Client agrees that the Cisco NGFWv Threat + URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603618 Cisco Firepower NGFW Virtual - Threat + Malware (1 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + Malware Defense (1 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (1 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + Malware Defense (1 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + Malware Defense running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (1 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + Malware Defense

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + Malware Defense .

End User License Agreement

Client agrees that the Cisco NGFWv Threat + Malware Defense software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603619 Cisco Firepower NGFW Virtual - Threat + Malware (100 Mbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + Malware Defense (100 Mbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (100 Mbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + Malware Defense (100 Mbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + Malware Defense running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (100 Mbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + Malware Defense

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + Malware Defense .

End User License Agreement

Client agrees that the Cisco NGFWv Threat + Malware Defense software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603620 Cisco Firepower NGFW Virtual - Threat + Malware (3 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + Malware Defense (3 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (3 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + Malware Defense (3 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + Malware Defense running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (3 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + Malware Defense

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + Malware Defense .

End User License Agreement

Client agrees that the Cisco NGFWv Threat + Malware Defense software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603621 Cisco Firepower NGFW Virtual - Threat + Malware (5 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + Malware Defense (5 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (5 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + Malware Defense (5 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + Malware Defense running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (5 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements

will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + Malware Defense

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + Malware Defense .

End User License Agreement

Client agrees that the Cisco NGFWv Threat + Malware Defense software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603622 Cisco Firepower NGFW Virtual - Threat + Malware (10 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + Malware Defense (10 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (10 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + Malware Defense (10 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + Malware Defense running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (10 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + Malware Defense

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + Malware Defense .

End User License Agreement

Client agrees that the Cisco NGFWv Threat + Malware Defense software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603623 Cisco Firepower NGFW Virtual - Threat + Malware (16 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + Malware Defense (16 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (16 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + Malware Defense (16 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + Malware Defense running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (16 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + Malware Defense

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request

support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + Malware Defense .

End User License Agreement

Client agrees that the Cisco NGFWv Threat + Malware Defense software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603624 Cisco Firepower NGFW Virtual - Threat + Malware + URL (100 Mbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + Malware Defense + URL (100 Mbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (100 Mbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + Malware Defense + URL (100 Mbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + Malware Defense + URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (100 Mbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file

control, and Security Intelligence filtering
- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies
- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + Malware Defense + URL

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat + URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all

tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + Malware Defense + URL.

End User License Agreement

Client agrees that the Cisco NGFWv Threat + Malware Defense + URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603625 Cisco Firepower NGFW Virtual - Threat + Malware + URL (3 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + Malware Defense + URL (3 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (3 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + Malware Defense + URL (3 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + Malware Defense + URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (3 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies
- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches

Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + Malware Defense + URL

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat + URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + Malware Defense + URL.

End User License Agreement

Client agrees that the Cisco NGFWv Threat + Malware Defense + URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603626 Cisco Firepower NGFW Virtual - Threat + Malware + URL (5 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + Malware Defense + URL (5 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (5 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + Malware Defense + URL (5 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + Malware Defense + URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (5 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies
- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a

time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + Malware Defense + URL

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat + URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + Malware Defense + URL.

End User License Agreement

Client agrees that the Cisco NGFWv Threat + Malware Defense + URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603627 Cisco Firepower NGFW Virtual - Threat + Malware + URL (10 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + Malware Defense + URL (10 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (10 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + Malware Defense + URL (10 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + Malware Defense + URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (10 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies
- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + Malware Defense + URL

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat + URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + Malware Defense + URL.

End User License Agreement

Client agrees that the Cisco NGFWv Threat + Malware Defense + URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603628 Cisco Firepower NGFW Virtual - Threat + Malware + URL (16 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - Threat + Malware Defense + URL (16 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (16 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - Threat + Malware Defense + URL (16 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual Threat + Malware Defense + URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (16 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies
- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + Malware Defense + URL

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat + URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + Malware Defense + URL.

End User License Agreement

Client agrees that the Cisco NGFWv Threat + Malware Defense + URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603629 Cisco Firepower NGFW Virtual - URL (1 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - URL (1 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (1 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - URL (1 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (1 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for URL

The following NGFW Support Services will be performed upon Client request:

- Client-identified moves/adds/changes and deletions relating to URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all

other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to URL.

End User License Agreement

Client agrees that the Cisco NGFWv URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603630 Cisco Firepower NGFW Virtual - URL (100 Mbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - URL (100 Mbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (100 Mbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - URL (100 Mbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (100 Mbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements

will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for URL

The following NGFW Support Services will be performed upon Client request:

- Client-identified moves/adds/changes and deletions relating to URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to URL.

End User License Agreement

Client agrees that the Cisco NGFWv URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603631 Cisco Firepower NGFW Virtual - URL (3 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - URL (3 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (3 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - URL (3 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (3 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for URL

The following NGFW Support Services will be performed upon Client request:

- Client-identified moves/adds/changes and deletions relating to URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to URL.

End User License Agreement

Client agrees that the Cisco NGFWv URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603632 Cisco Firepower NGFW Virtual - URL (5 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - URL (5 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (5 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - URL (5 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (5 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for URL

The following NGFW Support Services will be performed upon Client request:

- Client-identified moves/adds/changes and deletions relating to URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other

Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to URL.

End User License Agreement

Client agrees that the Cisco NGFWv URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603633 Cisco Firepower NGFW Virtual - URL (10 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - URL (10 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (10 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - URL (10 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (10 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)

Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for URL

The following NGFW Support Services will be performed upon Client request:

- Client-identified moves/adds/changes and deletions relating to URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to URL.

End User License Agreement

Client agrees that the Cisco NGFWv URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603634 Cisco Firepower NGFW Virtual - URL (16 Gbps) - Licenses and HA Management

The Cisco Firepower NGFW Virtual - URL (16 Gbps) - Licenses and HA Management service is an add-on to the Cisco Firepower NGFW Virtual - Base (16 Gbps) - Licenses and HA Management service

Cisco Firepower NGFW Virtual - URL (16 Gbps) - Licenses and HA Management is a combination of Company managed services for Cisco Firepower NGFW Virtual URL running on a pair of NGFW virtual appliances deployed in a high availability configuration (active/standby), separately contracted for license and management as Cisco Firepower NGFW Virtual - Base (16 Gbps) - Licenses and HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for URL

The following NGFW Support Services will be performed upon Client request:

- Client-identified moves/adds/changes and deletions relating to URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to URL.

End User License Agreement

Client agrees that the Cisco NGFWv URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603872 Cisco Firepower Single NGFW Virtual - Base (1 Gbps) - Licenses and Non-HA Management

The Cisco Firepower Single NGFW Virtual - Base (1 Gbps) - Licenses and Non-HA Management service is a combination of Company managed services for a single NGFW virtual appliance deployed in a high availability configuration and Cisco software

licensing for a single Cisco Firepower NGFW Virtual - Base (1 Gbps) for the purpose of running a managed Cisco Firepower NGFW Virtual, Non-HA firewall with Base on virtualized infrastructure provided by Client or contracted to be provided by Company.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv)

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Base NGFWv includes Application Visibility and Control (AVC) to reduce the potential surface area of attacks through granular control of thousands of applications and enforces mobile, social, and other acceptable use policies

Performance Specifications for NGFWv

Refer to https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw-virtual/threat-defense-virtual-ngfwv-ds.html

VPN peers are not included with this ItemID, but are available and can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Firewall Management

- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
  - Local Database
  - Lightweight Directory Access Portal (LDAP)
  - Authentication, Authorization and Accounting (AAA)
  - Active Directory (AD)
  - Multifactor authentication (MFA)
  - Security Information and event Management (SIEM)
- Remote access VPN management
  - Deployment and support of remote access VPN management vendor software including:
    - Group policy definitions
    - External user database authentication integration
    - Certificate management
    - Client VPN access utilizing Cisco client software
  - Site-to-site VPN management
    - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
    - Troubleshooting / support of VPN tunnel establishment
- Vendor-provided NGFW policy updates (application control)
- Schedule standard reports (make recipient modifications if necessary)
- Vendor firewall management system and associated computing resources

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against

Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Base

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Base
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Base
- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation, and reporting
- Data breach investigation and reporting

- Security gap analysis
- Threat intelligence collection and analysis

Virtualization Platform

Provide a virtualization platform to host the virtual Cisco Firepower NGFW and the firewall management system

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide console access to the OS
- Provide Internet connection for usage metering purposes

End User License Agreement

Client agrees that the Cisco NGFWv Base software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603873 Cisco Firepower Single NGFW Virtual - Base (100 Mbps) - Licenses and Non-HA Management

The Cisco Firepower Single NGFW Virtual - Base (100 Mbps) - Licenses and Non-HA Management service is a combination of Company managed services for a single NGFW virtual appliance deployed in a high availability configuration and Cisco software licensing for a single Cisco Firepower NGFW Virtual - Base (100 Mbps) for the purpose of running a managed Cisco Firepower NGFW Virtual, Non-HA firewall with Base on virtualized infrastructure provided by Client or contracted to be provided by Company.

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv)

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Base NGFWv includes Application Visibility and Control (AVC) to reduce the potential surface area of attacks through granular control of thousands of applications and enforces mobile, social, and other acceptable use policies

Performance Specifications for NGFWv

Refer to https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw-virtual/threat-defense-virtual-ngfwv-ds.html

VPN peers are not included with this ItemID, but are available and can be purchased from Company under a separate ItemID.

Company's Responsibilities and Included Features

Firewall Management

- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
    - Local Database

        - Lightweight Directory Access Portal (LDAP)
        - Authentication, Authorization and Accounting (AAA)
        - Active Directory (AD)
        - Multifactor authentication (MFA)
        - Security Information and event Management (SIEM)
    - Remote access VPN management
        - Deployment and support of remote access VPN management vendor software including:
            - Group policy definitions
            - External user database authentication integration
            - Certificate management
            - Client VPN access utilizing Cisco client software
        - Site-to-site VPN management
            - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
            - Troubleshooting / support of VPN tunnel establishment
    - Vendor-provided NGFW policy updates (application control)
    - Schedule standard reports (make recipient modifications if necessary)
    - Vendor firewall management system and associated computing resources

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Base

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Base
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request

support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Base
- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation, and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

Virtualization Platform

Provide a virtualization platform to host the virtual Cisco Firepower NGFW and the firewall management system

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide console access to the OS
- Provide Internet connection for usage metering purposes

End User License Agreement

Client agrees that the Cisco NGFWv Base software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603874 Cisco Firepower Single NGFW Virtual - Threat + Malware + URL (1 Gbps) - Licenses and Non-HA Management

The Cisco Firepower Single NGFW Virtual - Threat + Malware Defense + URL (1 Gbps) - Licenses and Non-HA Management service is an add-on to the Cisco Firepower Single NGFW Virtual - Base (1 Gbps) - Licenses and Non-HA Management service

Cisco Firepower Single NGFW Virtual - Threat + Malware Defense + URL (1 Gbps) - Licenses and Non-HA Management is a combination of Company managed services for Cisco Firepower Single NGFW Virtual Threat + Malware Defense + URL running on a single NGFW virtual appliance deployed in a high availability configuration, separately contracted for license and management as Cisco Firepower Single NGFW Virtual - Base (1 Gbps) - Licenses and Non-HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies
- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + Malware Defense + URL

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat + URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents

- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + Malware Defense + URL.

End User License Agreement

Client agrees that the Cisco NGFWv Threat + Malware Defense + URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603875 Cisco Firepower Single NGFW Virtual - Threat + Malware + URL (100 Mbps) - Licenses and HA Management

The Cisco Firepower Single NGFW Virtual - Threat + Malware Defense + URL (100 Mbps) - Licenses and Non-HA Management service is an add-on to the Cisco Firepower Single NGFW Virtual - Base (100 Mbps) - Licenses and Non-HA Management service

Cisco Firepower Single NGFW Virtual - Threat + Malware Defense + URL (100 Mbps) - Licenses and Non-HA Management is a combination of Company managed services for Cisco Firepower Single NGFW Virtual Threat + Malware Defense + URL running on a single NGFW virtual appliance deployed in a high availability configuration, separately contracted for license and management as Cisco Firepower Single NGFW Virtual - Base (100 Mbps) - Licenses and Non-HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering
- URL subscriptions provide URL filtering to limit access to websites by permitting or denying access based on defined policies
- Advanced malware protection provides threat intelligence, malware analysis and ability to continuously monitor file behavior and traffic.

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat + Malware Defense + URL

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat + URL
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat + Malware Defense + URL.

End User License Agreement

Client agrees that the Cisco NGFWv Threat + Malware Defense + URL software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603876 Cisco Firepower Single NGFW Virtual - Threat (1 Gbps) - Licenses and Non-HA Management

The Cisco Firepower Single NGFW Virtual - Threat (1 Gbps) - Licenses and Non-HA Management service is an add-on to the Cisco Firepower Single NGFW Virtual - Base (1 Gbps) - Licenses and Non-HA Management service

Cisco Firepower Single NGFW Virtual - Threat (1 Gbps) - Licenses and Non-HA Management is a combination of Company managed services for Cisco Firepower Single NGFW Virtual Threat running on a single NGFW virtual appliance deployed in a high availability configuration, separately contracted for license and management as Cisco Firepower Single NGFW Virtual - Base (1 Gbps) - Licenses and Non-HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat .

End User License Agreement

Client agrees that the Cisco NGFWv Threat software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

603877 Cisco Firepower Single NGFW Virtual - Threat (100 Mbps) - Licenses and Non-HA Management

The Cisco Firepower Single NGFW Virtual - Threat (100 Mbps) - Licenses and Non-HA Management service is an add-on to the Cisco Firepower Single NGFW Virtual - Base (100 Mbps) - Licenses and Non-HA Management service

Cisco Firepower Single NGFW Virtual - Threat (100 Mbps) - Licenses and Non-HA Management is a combination of Company managed services for Cisco Firepower Single NGFW Virtual Threat running on a single NGFW virtual appliance deployed in a high availability configuration, separately contracted for license and management as Cisco Firepower Single NGFW Virtual - Base (100 Mbps) - Licenses and Non-HA Management

Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Cisco Firepower Next-Generation Firewall Virtual (NGFWv) Add-on features

NGFWv offers threat protection features and centralized management for security effectiveness and visibility across physical and virtual workloads.

- Threat subscription additionally includes Intrusion Prevention System (IPS) for intrusion detection and prevention, file control, and Security Intelligence filtering

Company's Responsibilities and Included Features

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Identification of moves/adds/changes and deletions to be performed by Company relating to Threat .

End User License Agreement

Client agrees that the Cisco NGFWv Threat software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco

Intellectual Property rights including pursuing an action against any breaching third parties.

604250 Cisco Firepower Single NGFW Management Only - Base + Threat + Malware

The Cisco Firepower NGFW Management Only - Base + Threat + Malware is a service intended for Client owned Cisco Firepower NGFW with Base + Threat + Malware licensing already installed. This will solely cover the management of the Cisco Firepower NGFW and will not include software licensing for the aforementioned device.

Company's Responsibilities and Included Features

Firewall Management

- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of remote access VPN management vendor software including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing Cisco client software
    - Site-to-site VPN management
        - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
        - Troubleshooting / support of VPN tunnel establishment
- Vendor-provided NGFW policy updates (application control)
- Schedule standard reports (make recipient modifications if necessary)
- Vendor firewall management software

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Base

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Base

- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

Support Services for Threat

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

Support Services for Malware Defense

The following NGFW Support Services will be performed upon Client request:

- Client-identified moves/adds/changes and deletions relating to Malware
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

,

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Identification of moves/adds/changes and deletions to be performed by Company.

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

Hardware Maintenance Coverage

- Procurement of hardware maintenance
- Provide contract numbers and phone numbers of applicable hardware maintenance service providers
- Ensure that Company is an authorized caller to maintenance service providers

Virtualization Platform

Provide a virtualization platform to host the virtual Cisco Firepower NGFW and the firewall management system

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide console access to the OS

Cisco NGFW Licensing

- Procure Cisco NGFW software and licensing for current version of Cisco NGFW
- Procure current software maintenance where applicable

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

,347.5,347.5,630.069,0.0%,630.069,630.069,44.85%, 23

606975 Cisco Umbrella Insights Subscriptions

Company's Responsibilities and Included Features

Licenses

Provide Cisco Umbrella Insights Licenses up to the quantity as stated in the Pricing Details above. Licenses will be provided on a monthly subscription basis.

Support Services for AMP

Upon Client request, escalate appropriate issues to Cisco TAC (Technical Assistance Center). Support services for Umbrella Insights are not included under this ItemID, but may be contracted under a separate ItemID.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware

and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless contracted separately with Company under this or another Executed Order, Client is responsible for the following:

Identification of moves/adds/changes and deletions to be performed by Company relating to Cisco Umbrella Insights

Except as provided above, all support services for Umbrella Insights.

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco Umbrella Insights software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

606976 Cisco Umbrella DNS E Subscriptions

Company's Responsibilities and Included Features

Licenses

Provide Cisco Umbrella DNS E Licenses up to the quantity as stated in the Pricing Details above. Licenses will be provided on a monthly subscription basis.

Support Services for AMP

Upon Client request, escalate appropriate issues to Cisco TAC (Technical Assistance Center). Support services for Umbrella DNS E are not included under this ItemID, but may be contracted under a separate ItemID.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company

and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless contracted separately with Company under this or another Executed Order, Client is responsible for the following:

Identification of moves/adds/changes and deletions to be performed by Company relating to Cisco Umbrella DNS E

Except as provided above, all support services for Umbrella DNS E.

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco Umbrella DNS E software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

606977 Cisco Umbrella DNS A Subscriptions

Company's Responsibilities and Included Features

Licenses

Provide Cisco Umbrella DNS A Licenses up to the quantity as stated in the Pricing Details above. Licenses will be provided on a monthly subscription basis.

Support Services for AMP

Upon Client request, escalate appropriate issues to Cisco TAC (Technical Assistance Center). Support services for Umbrella DNS A are not included under this ItemID, but may be contracted under a separate ItemID.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless contracted separately with Company under this or another Executed Order, Client is responsible for the following:

Identification of moves/adds/changes and deletions to be performed by Company relating to Cisco Umbrella DNS A

Except as provided above, all support services for Umbrella DNS A.

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco Umbrella DNS A software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

606978 Cisco Umbrella SIG E Subscriptions

Company's Responsibilities and Included Features

Licenses

Provide Cisco Umbrella SIG E Licenses up to the quantity as stated in the Pricing Details above. Licenses will be provided on a monthly subscription basis.

Support Services for AMP

Upon Client request, escalate appropriate issues to Cisco TAC (Technical Assistance Center). Support services for Umbrella SIG E are not included under this ItemID, but may be contracted under a separate ItemID.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless contracted separately with Company under this or another Executed Order, Client is responsible for the following:

Identification of moves/adds/changes and deletions to be performed by Company relating to Cisco Umbrella SIG E

Except as provided above, all support services for Umbrella SIG E.

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco Umbrella SIG E software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

606979 Cisco Umbrella SIG A Subscriptions

Company's Responsibilities and Included Features

Licenses

Provide Cisco Umbrella SIG A Licenses up to the quantity as stated in the Pricing Details above. Licenses will be provided on a monthly subscription basis.

Support Services for AMP

Upon Client request, escalate appropriate issues to Cisco TAC (Technical Assistance Center). Support services for Umbrella SIG A are not included under this ItemID, but may be contracted under a separate ItemID.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless contracted separately with Company under this or another Executed Order, Client is responsible for the following:

Identification of moves/adds/changes and deletions to be performed by Company relating to Cisco Umbrella SIG A

Except as provided above, all support services for Umbrella SIG A.

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco Umbrella SIG A software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

606980 Cisco Umbrella DLP Subscriptions

Company's Responsibilities and Included Features

Licenses

Provide Cisco Umbrella DLP Licenses up to the quantity as stated in the Pricing Details above. Licenses will be provided on a monthly subscription basis.

Support Services for AMP

Upon Client request, escalate appropriate issues to Cisco TAC (Technical Assistance Center). Support services for Umbrella DLP are not included under this ItemID, but may be contracted under a separate ItemID.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless contracted separately with Company under this or another Executed Order, Client is responsible for the following:

Identification of moves/adds/changes and deletions to be performed by Company relating to Cisco Umbrella DLP

Except as provided above, all support services for Umbrella DLP.

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco Umbrella DLP software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

606981 Cisco Umbrella CDFW Subscriptions

Company's Responsibilities and Included Features

Licenses

Provide Cisco Umbrella CDFW Licenses up to the quantity as stated in the Pricing Details above. Licenses will be provided on a monthly subscription basis.

Support Services for AMP

Upon Client request, escalate appropriate issues to Cisco TAC (Technical Assistance Center). Support services for Umbrella CDFW are not included under this ItemID, but may be contracted under a separate ItemID.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless contracted separately with Company under this or another Executed Order, Client is responsible for the following:

Identification of moves/adds/changes and deletions to be performed by Company relating to Cisco Umbrella CDFW

Except as provided above, all support services for Umbrella CDFW.

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

End User License Agreement

Client agrees that the Cisco Umbrella CDFW software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

608410 Cisco Firepower Single NGFW Management Only - Base + Threat

The Cisco Firepower NGFW Management Only - Base + Threat is a service intended for Client owned Cisco Firepower NGFW

with Base + Threat licensing already installed. This will solely cover the management of the Cisco Firepower NGFW and will not include software licensing for the aforementioned device.

Company's Responsibilities and Included Features

Firewall Management

- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of remote access VPN management vendor software including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing Cisco client software
    - Site-to-site VPN management
        - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
        - Troubleshooting / support of VPN tunnel establishment
- Vendor-provided NGFW policy updates (application control)
- Schedule standard reports (make recipient modifications if necessary)
- Vendor firewall management software

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Base

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Base
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

Support Services for Threat

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts, and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot NGFWv security incidents specific to Company managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

,

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Identification of moves/adds/changes and deletions to be performed by Company.

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

Hardware Maintenance Coverage

- Procurement of hardware maintenance
- Provide contract numbers and phone numbers of applicable hardware maintenance service providers

- Ensure that Company is an authorized caller to maintenance service providers

Virtualization Platform

Provide a virtualization platform to host the virtual Cisco Firepower NGFW and the firewall management system

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide console access to the OS

Cisco NGFW Licensing

- Procure Cisco NGFW software and licensing for current version of Cisco NGFW
- Procure current software maintenance where applicable

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

,278.0,278.0,503.0552,0.0%,503.0552,503.0552,44.74%, 234

Category: Storage

500091 Economy Backup Service Setup

Company's Responsibilities and Included Features

- Backup agent installed and configured by Company on supported Operating Systems and Applications
- Exclusion of non-essential files such as recycle bin and A/V files to save space and prevent errors customizable during implementation
- Initial configuration of agent software and backend infrastructure components
- Provide support to service desk and service administrator personnel and act as an escalation point
- Last line of support before escalating to vendor support for product issues.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Runs backup and recovery
- Escalation point on the Client side
- Responsible internally for service

500149 Bronze - Block level storage services (NextGen)

Company's Responsibilities and Included Features

- Present shared SAN space to hosted environment leveraging Company's shared SAN infrastructure
- Utilizes software-based Advanced Encryption Standard (AES) 256 encryption algorithm
- Redundancy provided by redundant SAN head units
- Tier III low data use disk presentation .1 IOPS/GB
- Administration of the SAN Storage Systems includes:
    - Backend disk storage management including:
        - RAID group configuration
        - Volume configuration

        - SAN: LUN provisioning
        - Monitoring and reporting of disk space usage
    - Triage and troubleshoot SAN/NAS infrastructure, performance and presentation issues -Global settings/configuration management including LUN definitions
    - SAN: Dynamic/Redundant path presentation. (may require proprietary multi-path software) (if applicable)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Data Backup (unless covered under additional Company services)

600267 Dedicated Nimble Storage

Company's Responsibilities and Included Features

- Present SAN space to hosted environment leveraging Company's Client dedicated SAN infrastructure.
- Utilizes software-based Advanced Encryption Standard (AES) 256 encryption algorithm.
- Tier II general workload performance disk presentation, limited to 120,000 IOPs per SAN array.
- Administration of the SAN Storage Systems includes:
    - RAID group configuration.
    - Volume configuration.
    - SAN: LUN provisioning.
    - Monitoring and reporting of disk space usage.
    - Storage replication administration.
- Triage and troubleshoot SAN/NAS infrastructure, performance and presentation issues.
- Global settings/configuration management including LUN definitions.
- SAN: Dynamic/Redundant path presentation. (may require proprietary multi-path software) (if applicable)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Data Backup.

600276 Array based snapshot service (NextGen Silver) - per 100GB

Company's Responsibilities and Included Features

- Configure array based snapshot service based on Client provided snapshot frequency and retention criteria
- Troubleshoot errors associated with snapshot service
- Provide monthly reporting based on actual consumed snapshot storage on array
- Service is metered and billed based on max snapshot space usage per month

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of changes to snapshot criteria
- Review monthly sanpshot usage data

601843 ReliaCloud ELASTIC Files Service

Company's Responsibilities and Included Features

ReliaCloud ELASTIC Files Service (ELASTIC Files) offers a software-defined scale-out file storage solution designed to address a wide range of use cases, including support for Linux and Windows home directories, user profiles and department shares.

Features

- Server Message Block (SMB) versions 2 and 3 (SMBv2 and SMB v3) support
- Network File System (NFS) versions 3 and 4 (NFSv3 and NFSv4) support
- Multiprotocol support
- High availability architecture
- Self-service file restoration
- Hot workloads performance tier

ELASTIC Files is accessible within and between ReliaCloud data center locations and supports VPN based connections over the Internet (requires additional Company VPN service).

Data Protection:

Elastic Files is locally protected with two copies of your data within the system, plus any optional snapshots stored locally. ELASTIC Files may additionally be replicated to another ReliaCloud data center location (requires additional item ID).

Metered Service:

- This service is metered
- The quantity of ELASTIC Files storage space is comprised of replicated stored data, file storage and snapshot space
- The quantity is measured hourly
- Usage for a month is the average of the hourly measurements captured during that month.

Managed Service:

ELASTIC Files is a Company managed service providing support administration of the following functions:

- File Server Management
    - Encryption settings
- Share and Export Management
    - Creating file shares
    - Creating exports
    - Multiprotocol support
- Domain Configuration Management
    - Domain joining
    - Updating Domain Name System (DNS) entries
    - Disjoint domain management
- Directory and User Management
    - Updating files directory services
    - Management of user mappings
    - Managing user roles
    - Management of user quotas
- Data Recovery Management
    - Management of protection domain and snapshot schedule
    - Configuration of self-service restore (SSR) and snapshot schedule parameters

ELASTIC Files Triage and Troubleshooting:

- Triage of ELASTIC Files system incidents
- Troubleshoot and work to resolve ELASTIC Files system incidents
- Document ELASTIC Files system issues and errors

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents

6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Manage end user files shares, access management and usage
- Migration of files data on to and off of the Cluster
- Open necessary network and firewall ports to provide Company access to Management VMs
- If applicable, provide VPN termination point for Company to access Client s environment
- If applicable subscribe to Company services to facilitate WAN or VPN access, such as but not limited to VPN services and Internet bandwidth, cross-connections, or circuit termination services
- Provide Company with a snapshot policy
- Execute file level self-service restorations
- Provide a directory service and credentials to integrate into the ELASTIC Files Protection Service

601844 ReliaCloud ELASTIC Files Protection Service

Company's Responsibilities and Included Features

ReliaCloud ELASTIC Files Protection Service (ELASTIC Files Protection) provides a replication target (availability zone) for Company s ReliaCloud ELASTIC Files Service, ReliaCloud EDGE Nodes or clients running Nutanix Files software within their environments.

Elastic File Protection features:

- Nutanix Files based service
- Asynchronous replication with a 60-minute recovery point objective (RPO)
- Storage space to land Client-defined, scheduled and replicated Nutanix Files snapshots
- The ability to activate (power-on) the replicated snapshots into the Company hosted environment

Powered-On / Powered-Off status:

ELASTIC Files Protection covers File Server Virtual Machine(s) (FSVM) and their associated data (Replicated Set) that are replicated to ReliaCloud ELASTIC in a powered-off state and remain powered off until powered on. In order to utilize the Replicated Set, Client must request Company power it on. Client may request the Replicated Set to be powered on for testing, fail-over, long-term production or other purposes. During a fail-over event, replication services will not be available until another fail-over or fail-back target is agreed to by Company and Client and setup by Company to restart replication services.

Powered-On Features:

- Server Message Block (SMB) versions 2 and 3 (SMB v2 and SMB v3) support
- Network File System (NFS) versions 3 and 4 (NFSv3 and NFSv4) support
- Multiprotocol support
- High availability architecture
- Self-service file restoration
- Hot workloads performance tier
- Files are locally protected with two copies of Client s data within the system, plus any optional snapshots stored locally.
- ELASTIC Files Protection provides scalable file storage based upon a per GiB/hour consumption model.
- ELASTIC Files Protection is accessible within and between ReliaCloud data center locations and can support VPN based connections over the Internet (requires additional Company VPN service).

Metered Service:

- This service is metered
- The quantity of ELASTIC Files storage space is comprised of replicated stored data, file storage and snapshot space
- The quantity is measured hourly
- Usage for a month is the average of the hourly measurements captured during that month.

Managed Service:

ELASTIC Files Protection is a Company managed service providing support administration of the following functions:

- File Server Management
  - Encryption settings
- Share and Export Management
  - Creating file shares
  - Creating exports
  - Multiprotocol support
- Domain Configuration Management
  - Domain joining
  - Updating Domain Name System (DNS) entries
  - Disjoint domain management
- Directory and User Management
  - Updating files directory services
  - Management of user mappings
  - Managing user roles
  - Management of user quotas
- Data Recovery Management
  - Management of protection domain and snapshot schedule
  - Configuration of self-service restore (SSR) and snapshot schedule parameters

ELASTIC Files Protection Triage and Troubleshooting

- Triage of ELASTIC Files Protection incidents
- Troubleshoot and work to resolve ELASTIC Files Protection incidents
- Document ELASTIC Files Protection issues and errors This service is metered

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Manage end user files shares, access management and usage
- Migration of files data on to and off of the Cluster
- Open necessary network and firewall ports to provide Company access to Management VMs
- If applicable, provide VPN termination point for Company to access Client s environment

- If applicable, subscribe to Company services to facilitate WAN or VPN access such as but not limited to VPN services and Internet bandwidth, cross-connections, or circuit termination services
- Provide Company with a snapshot policy and snapshot replication schedule
- Provide Company with service account on Client domain controller(s)
- Allow Company to modify DNS records to support ELASTIC Files Services
- Execute file level self-service restorations
- Provide a directory service and credentials to integrate into the ELASTIC Files Protection Service

For Client owned infrastructure

- Subscribe to Company Nutanix Managed Files Service
- Asynchronous replication must be leveraged
- RPOs no smaller than 60-minutes
- Nutanix AOS versions must match between Client owned cluster and the ReliaCloud ELASTIC Files Protection Service
- Client must be on either Nutanix AHV or VMware ESXi hypervisors within their cluster to be protected

601874 ReliaCloud ELASTIC Objects

Definitions

S3: The term used to describe Amazon Web Services Simple Storage Service (AWS S3) Interface is now used synonymously for an object service. S3 is also used to describe the object API which you use to interact with an Object Store.

REST API: A RESTful API is an architectural style for an application program interface (API) that uses HTTP requests to access and use data. That data can be used to GET, PUT, POST and DELETE data types, which refers to the reading, updating, creating and deleting of operations concerning resources.

Object Store: Also known as object-based storage is a computer data storage architecture that manages data as objects, as opposed to other storage architectures like file systems which manages data as a file hierarchy, and block storage which manages data as blocks within sectors and tracks.

Object: The actual unit (blob) of storage and the item interfaced by using the REST API (GET or PUT).

Bucket: An organizational unit exposed to the users and that contains the objects. A deployment may have one or more buckets.

Company's Responsibilities and Included Features

ReliaCloud ELASTIC Objects Service (ELASTIC Objects) offers a software-defined Object Store Service. This service is designed with an Amazon Web Services Simple Storage Service (AWS S3) compatible REST API interface capable of handling petabytes of unstructured and machine-generated data. ELASTIC Objects storage solution is designed to address a wide range of use cases not limited to; backup, long-term data retention, and data storage for cloud-native applications using standard S3 APIs.

Features:

- Standard S3 API compatible interface
- Multipart upload API
- Object life cycle policies
- Quota storage and bucket creation quota policies
- Buckets for static web site hosting
- High availability architecture

ELASTIC Objects is accessible as an over the Internet service.

Data Protection:

- ELASTIC Objects is locally protected with two copies of your data within the system
- ELASTIC Objects leverages data at rest encryption

Object versioning

- ELASTIC Objects may additionally have Client Buckets set to an immutable policy-based state leveraging write-once-read-many (WORM) to protect object and meta data (requires additional item ID).
- ELASTIC Objects may additionally be replicated to another ReliaCloud data center location (requires additional item ID)

Service Meter Definition:

- This service is metered
- The quantity of ELASTIC Objects storage space is comprised of amount of data contained with the Bucket(s) presented to Client.
- Usage for a month is the average of the hourly measurements captured during that month.

Management Activities:

ELASTIC Objects is a Company managed service providing administration of the following functions:

- Container Management
    - Data at rest encryption settings
- Bucket Management
    - Bucket creation
    - Per Client request:
        - Object life cycle policy creation and or modification
        - Enable/disable object versioning
        - Configuration for static website hosting and Cross-Origin Resource Sharing (CORS)
- User Management
    - Role based access control setup, definition and modification
    - User creation and key provisioning
    - If requested by Client, set user quota policies

ELASTIC Objects Triage and Troubleshooting:

- Triage of ELASTIC Objects system incidents
- Troubleshoot and work to resolve ELASTIC Objects system incidents
- Document ELASTIC Objects system issues and errors

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Manage end user Buckets access management and usage
- Migration of Objects data into and off of service
- Provide Company with any policy definitions as identified above

Definitions

Bucket: An organizational unit exposed to the users and contains the objects. A deployment may have one or more buckets.

Object: The actual unit (blob) of storage and the item interfaced by using the REST API (GET or PUT).

Object Store: Also known as object-based storage is a computer data storage architecture that manages data as objects, as opposed to other storage architectures like file systems which manages data as a file hierarchy, and block storage which manages data as blocks within sectors and tracks.

REST API: A RESTful API is an architectural style for an application program interface (API) that uses HTTP requests to access and use data. That data can be used to GET, PUT, POST and DELETE data types, which refers to the reading, updating, creating and deleting of operations concerning resources.

S3: The term used to describe Amazon Web Services Simple Storage Service (AWS S3) Interface is now used synonymously for an object service. S3 is also used to describe the object API which you use to interact with an Object Store.

WORM: Write Once Read Many, a term used to describe a storage protection technology to prevent deletion or modification of the data and its associated meta data.

Company's Responsibilities and Included Features

ReliaCloud ELASTIC Objects Service (ELASTIC Objects) offers a software-defined Object Store Service. This service is designed with an Amazon Web Services Simple Storage Service (AWS S3) compatible REST API interface capable of handling petabytes of unstructured and machine-generated data. ELASTIC Objects storage solution is designed to address a wide range of use cases not limited to; backup, long-term data retention, multi-cloud snapshot retention and data storage for cloud-native applications using standard S3 APIs. ELASTIC Objects is accessible as an over the Internet service.

Features:

Bucket Object storage

- Objects Browser, a user interface that allows the end user to perform Bucket and Object level operations.
- Standard S3 API compatible interface
- Multipart upload API
- Object life cycle policies Quota storage and bucket creation quota policies
- High availability architecture
- Erasure-Coding (EC-X) space savings technology

Bucket Replication

- Streaming Asynchronous unidirectional replication of a ReliaCloud ELASTIC Objects source Bucket
- High-speed wide area network for object replication
- Ability to perform reads and write operations on the remote Bucket

WORM Data Protection

- Entire Bucket WORM Protection for the data and meta data
- Policy based retention period
- Versioning option, not enabled by default
- Grace period of 24 hours after policy enablement, after which the policy is permanent
- Retention polices cannot be decreased only extended

CORS/Web Site static hosting

- Static content website hosting
- Website URL redirection
- Support for index and error page
- Cross-Origin resource sharing

Versioning option, not enabled by default

Data Protection:

- Every interaction with ELASTIC Objects is authenticated
- An access key ID, and associated secret key are provided
- Data transmission is exclusively over HTTPS: 443
- ELASTIC Objects is locally protected with two copies of your data within the system
- ELASTIC Objects leverages data at rest encryption
- Optional use of Object level legal hold
- Optional use of Object versioning, not enabled by default
- ELASTIC Objects may additionally have Client Buckets set to an immutable policy-based state leveraging write-once-read-many (WORM) to protect object and meta data
- ELASTIC Objects may additionally be replicated to another ReliaCloud data center location

Internet Data Egress

- Internet data ingress is free of charge

Service Meter Definition Objects Storage

- This service is metered
- The quantity of ELASTIC Objects storage space is comprised of amount of data contained with the Bucket(s) presented to Client.
- The quantity is measured hourly
- Usage for a month is the average of the hourly measurements captured during that month.

Management Activities:

ELASTIC Objects is a Company managed service providing administration of the following functions:

- Container Management
    - Data at rest encryption settings
- Bucket Management
    - Bucket creation
    - Per Client request:
        - Object life cycle policy creation and or modification
        - Enable/disable object versioning
    - Triage of ELASTIC Objects system incidents
    - Troubleshoot and work to resolve ELASTIC Objects system incidents
    - Document ELASTIC Objects system issues and errors

Bucket Replication is a Company managed service providing administration of the following functions:

- Enablement of Bucket Replication
- Define availability zone for remote Bucket
- Creation of replication rules between Buckets
- Assignment of Bucket access permission on the Source Bucket
- Replication Management
    - Adjustments to replication rules per Client request
    - Define performance monitoring and alerting per Company best practices

WORM Buckets are a Company managed service providing administration of the following functions:

- Per Client Request
    - Creation of Bucket and application of WORM setting
    - Apply WORM retention policy per Client specification

CORS/Web Buckets are a Company managed service providing administration of the following functions:

- Per Client Request
  - Creation of Bucket and application of CORS and or Website hosting settings
- Triage of CORS/Web Buckets Replication system incidents
- Troubleshoot and work to resolve CORS/Web Buckets Replication system incidents
- Document CORS/Web Buckets Replication system issues and errors
- Configuration for static website hosting and Cross-Origin Resource Sharing (CORS)

User Management

- Role based access control setup, definition and modification
- User creation and key provisioning
- If requested by Client, set user quota policies

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Manage end user Buckets access management and usage
- Migration of Objects data into and off of service
- Provide Company with any policy definitions as identified above
- Troubleshoot Client or third-party code that leverages the ELASTIC Objects S3 API.

Prohibited Use - Content Delivery Network (CDN) Restrictions:

Client acknowledges and agrees that the Object Storage Service provided under this Agreement is not intended to function as, nor may it be used as, a Content Delivery Network (CDN). Accordingly, Client shall not:

- Use the Object Storage Service primarily for the purpose of distributing, caching, accelerating, or serving high-volume, publicly accessible static or dynamic content, including but not limited to images, videos, software downloads, streaming media, or other content that is typically delivered via a CDN.
- Configure or utilize the Object Storage Service in a manner that results in excessive outbound data transfer, network congestion, or disproportionate resource consumption relative to standard storage operations.
- Implement edge caching, global replication, or other performance-enhancing techniques intended to mimic or replace the functionality of a traditional CDN.
- Allow third parties to directly access or retrieve stored content in a manner that circumvents reasonable access controls or effectively offloads CDN-like services onto the Object Storage Service.

In the event of a violation of this restriction, the Company reserves the right to take appropriate action, including but not limited to rate limiting, throttling, suspending, or terminating the Client s access to the Object Storage Service. Provider further reserves the right to charge additional fees based on excessive outbound data usage if such activity is detected.

Category: Virtual Desktop

602106 ReliaCloud EDGE EUC Node 104 - HMAHV

Definition

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

EUC: End User Compute services also known as Virtual Desktop Infrastructure (VDI), Desktop as a Service (DaaS) and virtual application hosting. EUC is a solution for services which commonly replace the conventional physical desktop with a virtualized platform.

GPU: Graphics processing unit (GPU) is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE EUC Node 104 - HMAHV (EDGE EUC Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE EUC Nodes minimally belong to a Cluster configured with at least three (3) EDGE EUC Nodes. EDGE EUC Nodes are dedicated to the Client for their exclusive use.

Node physical specifications

Company will provide an EDGE EUC Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 6248R (3.0 GHz, 24 cores), 48 cores total
- 1536 GB RAM
- Hybrid performance disk configuration consisting of 24TB HDD and 7.68TB SSD
- GPU capable, zero GPUs installed

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of EUC and other workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Software Specifications

- Nutanix AOS Pro
- Nutanix Prism Pro
- Nutanix Data at Rest Encryption
- NVIDIA software driver

AOS Administration

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering

        - Inline compression
        - Inline performance deduplication
        - Online Cluster growth
        - Compression
        - Deduplication
        - Erasure coding (EC-X) *
    - Infrastructure Resilience
        - Data path redundancy
        - Tunable redundancy factor
    - Security
        - Client authentication
        - Cluster lockdown
        - Data-at-rest encryption (software-based and self-encrypting drives)
    - Management and Analytics
        - Prism Central and Prism Elements
        - Pulse
        - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals. Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Block and Node Maintenance Management

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones

        - VM-centric Storage QoS
        - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Co-administration

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
    - Cluster and VM performance and analysis
    - Cluster and health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection and recovery policies

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

602108 ReliaCloud EDGE EUC Node 124 - HMAHV

Definition

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

EUC: End User Compute services also known as Virtual Desktop Infrastructure (VDI), Desktop as a Service (DaaS) and virtual application hosting. EUC is a solution for services which commonly replace the conventional physical desktop with a virtualized platform.

GPU: Graphics processing unit (GPU) is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE EUC Node 124 - HMAHV (EDGE EUC Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. EDGE EUC Nodes minimally belong to a Cluster configured with at least three (3) EDGE EUC Nodes. EDGE EUC Nodes are dedicated to the Client for their exclusive use.

Node physical specifications

Company will provide an EDGE EUC Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 6248R (3.0 GHz, 24 cores), 48 cores total
- 1536 GB RAM
- Hybrid performance disk configuration consisting of 24TB HDD and 7.68TB SSD
- Two (2) NVIDIA T4 GPU card installed

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of EUC and other workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Software Specifications

- Nutanix AOS Pro
- Nutanix Prism Pro
- Nutanix Data at Rest Encryption
- NVIDIA software driver

AOS Administration

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all

configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals. Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Block and Node Maintenance Management

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

GPU Administration

- Manage and maintain NVIDIA Grid Licensing
    - Manage AOS Cluster drivers for NVIDIA grid GPU virtualization software

GPU Triage and Troubleshooting

- Triage of GPU system incidents
- Troubleshoot and work to resolve GPU system incidents
- Document GPU system issues and errors

Co-administration

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
    - Cluster and VM performance and analysis
    - Cluster and health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection and recovery policies

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment
- Subscribe to company s services for NVIDIA Grid licensing services

Third Party Utilities and Applications

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.
- Client agrees that NVIDIA offerings provided herein are subject to the NVIDIA End User License Agreement for GPU available https://images.nvidia.com/content/pdf/grid/support/enterprise-eula-grid-and-amgx-supplements.pdf which is hereby incorporated into this SOW in full.

602753 ReliaCloud EDGE Node EUC.4807HG0.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

EUC: End User Compute services also known as Virtual Desktop Infrastructure (VDI), Desktop as a Service (DaaS) and virtual application hosting. EUC is a solution for services which commonly replace the conventional physical desktop with a virtualized platform.

GPU: Graphics processing unit (GPU) is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE EUC.4807HG4.A (EDGE VDI Only Node) service is comprised of hardware and a base level of management services for the Nutanix AOS and Nutanix AHV. Nutanix software is a contracted separately under additional Company ItemIDs. EDGE VDI Only Nodes are licensed only for virtual desktop virtual machines (VMs), and those compute workloads that directly support the virtual desktops. EDGE VDI Only Nodes minimally belong to a Cluster configured with at least three (3) EDGE VDI Only Nodes. EDGE VDI Only Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE VDI Only Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 6342 (2.8 GHz, 24 cores), 48 cores total
- 1536 GB RAM
- Hybrid performance disk configuration consisting of 24TB HDD and 7.68TB SSD
- GPU capable, zero GPUs installed

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect usable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of EUC and other workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Software Specifications:

- None - contracted separately with additional ItemIDs

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse

- Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals. Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
  - Virtual Machine (VM) centric snapshots and clones
  - VM-centric Storage QoS
  - VM Flash Mode
- Data Protection
  - Application consistent snapshots
  - Local snapshots
  - Self-service restores
  - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
  - VM management. VM s operating system management and application management is specifically excluded from this scope.
  - VM automated resource scheduling
  - VM affinity rules
  - Virtual network configuration
  - Host profiles
  - VM high availability
  - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
  - Cluster and VM performance and analysis
  - Cluster and health and availability
  - Cluster capacity and trend info
  - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
  - Create, delete and modify VMs
  - Execute snapshots and restorations
  - Add VMs to catalog
  - Import, add, create and delete images to catalog
  - Create and modify data protection and recovery policies

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Contract for company Nutanix AOS VDI Per VM License Service

- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan;

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.

- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

602758 ReliaCloud EDGE Node EUC.4807HG5.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

EUC: End User Compute services also known as Virtual Desktop Infrastructure (VDI), Desktop as a Service (DaaS) and virtual application hosting. EUC is a solution for services which commonly replace the conventional physical desktop with a virtualized platform.

GPU: Graphics processing unit (GPU) is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE EUC.4807HG4.A (EDGE VDI Only Node) service is comprised of hardware and a base level of management services for the Nutanix AOS and Nutanix AHV. Nutanix software is a contracted separately under additional Company ItemIDs. EDGE VDI Only Nodes are licensed only for virtual desktop virtual machines (VMs), and those compute workloads that directly support the virtual desktops. EDGE VDI Only Nodes minimally belong to a Cluster configured with at least three (3) EDGE VDI Only Nodes. EDGE VDI Only Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE VDI Only Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 6342 (2.8 GHz, 24 cores), 48 cores total
- 1024 GB RAM
- Hybrid performance disk configuration consisting of 24TB HDD and 7.68TB SSD
- Five (5) NVIDIA T4 GPU cards installed

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect usable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of EUC and other workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Software Specifications:

- None - contracted separately with additional ItemIDs

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals. Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s

discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
  - Virtual Machine (VM) centric snapshots and clones
  - VM-centric Storage QoS
  - VM Flash Mode
- Data Protection
  - Application consistent snapshots
  - Local snapshots
  - Self-service restores
  - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
  - VM management. VM s operating system management and application management is specifically excluded from this scope.
  - VM automated resource scheduling
  - VM affinity rules
  - Virtual network configuration
  - Host profiles
  - VM high availability
  - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

GPU Administration:

- Manage and maintain NVIDIA Grid Licensing
    - Manage AOS Cluster drivers for NVIDIA grid GPU virtualization software

GPU Triage and Troubleshooting:

- Triage of GPU system incidents
- Troubleshoot and work to resolve GPU system incidents
- Document GPU system issues and errors

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
    - Cluster and VM performance and analysis
    - Cluster and health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection and recovery policies

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Contract for company Nutanix AOS VDI Per VM License Service
- Contract for company NVIDIA Virtual GPU Software services
- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan;

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.
- Client agrees that NVIDIA offerings provided herein are subject to the NVIDIA End User License Agreement for GPU available https://images.nvidia.com/content/pdf/grid/support/enterprise-eula-grid-and-amgx-supplements.pdf which is hereby incorporated into this SOW in full.

602766 ReliaCloud EDGE Node EUC.4807HG0.E

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

EUC: End User Compute services also known as Virtual Desktop Infrastructure (VDI), Desktop as a Service (DaaS) and virtual application hosting. EUC is a solution for services which commonly replace the conventional physical desktop with a virtualized platform.

GPU: Graphics processing unit (GPU) is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

VMware ESXi: VMware's hypervisor platform

Company's Responsibilities and Included Features

ReliaCloud EDGE EUC.4807HG0.E (EDGE VDI Only Node) service is comprised of hardware and a base level of management services for the Nutanix AOS and VMware ESXi. Nutanix and VMware software are contracted separately under additional Company ItemIDs. EDGE VDI Only Nodes are licensed only for virtual desktop virtual machines (VMs), and those compute workloads that directly support the virtual desktops. EDGE VDI Only Nodes minimally belong to a Cluster configured with at least three (3) EDGE VDI Only Nodes. EDGE VDI Only Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE VDI Only Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 6342 (2.8 GHz, 24 cores), 48 cores total

- 1536 GB RAM
- Hybrid performance disk configuration consisting of 24TB HDD and 7.68TB SSD
- NVIDIA T4 GPU capable, no GPUs installed

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect usable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of EUC and other workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Software Specifications:

- None - contracted separately with additional ItemIDs

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Nutanix Volumes Management
    - Creation of iSCSI volume group(s)
    - Management of volume groups
    - Management of client iSCSI initiators
    - Management of iSCSI data services
    - Configure Bare Metal Nodes for IP addressing
        - If Company determines it as a requirement, configuration and management of Challenge-Handshake Authentication (CHAP)
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor
- Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals. Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents

- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

VMware System Administration:

Company will support administration of the following base features of VMware ESXi:

- Perform preventative maintenance
- Perform emergency maintenance
- Provide performance tuning
- Perform server health checks
- Perform file system maintenance
- Provision Virtual Machines (VM)
- Manage basic vSwitch network
- Manage advanced network switching (i.e. VMware vDS or other vendor supported 3rd party switch)
- Manage basic vStorage network
- Manage VMware server through vCenter
- Manage vCenter application
- Administer built-in VMware dependency components
- Provide utilization reporting

LAN management of the virtual switch is specifically excluded from this scope of Services.

VMware ESXi Triage and Troubleshooting:

- Triage of VMware ESXi incidents
- Troubleshoot and work to resolve VMware ESXi system incidents
- Document VMware ESXi system issues and errors

VMware ESXi Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the ESXi software (including major upgrades) will be conducted at Company's discretion and in accordance with industry best practices.

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into vCenter and general visibility into the Cluster metrics and configuration settings such as as:
  - Cluster and VM performance and analysis
  - Cluster and health and availability
  - Cluster capacity and trend info
  - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
  - Create, delete and modify VMs
  - Execute snapshots and restorations
  - Add VMs to catalog
  - Import, add, create and delete images to catalog
  - Create and modify data protection and recovery policies

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Contract for Company Nutanix AOS VDI Per VM License Service
- Contract for Company NVIDIA Virtual GPU Software services
- Contract for Company VMware software services
- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party ESXi enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan;

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this

engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.
- Client agrees that NVIDIA offerings provided herein are subject to the NVIDIA End User License Agreement for GPU available https://images.nvidia.com/content/pdf/grid/support/enterprise-eula-grid-and-amgx-supplements.pdf which is hereby incorporated into this SOW in full.
- Client agrees, acknowledges, and understands that the actual manufacture of the VMware ESXi is by VMware, Inc. and its provision and performance may be subject to change as determined by VMware, Inc.
- Client agrees that VMware ESXi offerings provided herein are subject to the VMware Services End User License Agreement available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf and privacy policy located at https://www.vmware.com/help/privacy.html, which are hereby incorporated into this Statement of Work.

602829 Credit Applied From - ReliaCloud EUC Prepayment 602828

Company's Responsibilities and Included Features

Service Description

Client has elected to prepay for services provided by Company in the amount set forth by ItemID 602828 ReliaCloud EUC Prepayment - Quote 137033-3. Company will create a "Prepayment Balance" from the prepaid amount.

Client agrees that Company may deduct from your Prepayment Balance in monthly increments equal to the total of the balance divided by the length of the Contract Term in months for services rendered by Company.

If your Prepayment Balance is insufficient to cover any outstanding payment, we may charge both your Prepayment Balance and your second default payment method for Company provided services.

After deducting the monthly increment from the prepayment balance, company shall show that deducted amount as a credit on the associated month's invoice. Credits will be posted in arrears.

Client's prepayment does not provide Client with any ownership in part or whole of hardware or software associated with the delivery of Company provided services. Nor does the prepayment guarantee or govern make, model, feature set of underlying hardware, software an services. All Client elected, Company services are defined within the Service Catalog section of this agreement.

This service is not availabe for automatic renewal.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Have funded the Prepayment Balance with ItemID 602828

603551 ReliaCloud EDGE EUC.4807HGA16-2.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

EUC: End User Compute services also known as Virtual Desktop Infrastructure (VDI), Desktop as a Service (DaaS) and virtual application hosting. EUC is a solution for services which commonly replace the conventional physical desktop with a virtualized platform.

GPU: Graphics processing unit (GPU) is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE EUC.4807HGA16-2.A (EDGE VDI Only Node) service is comprised of hardware and a base level of management services for the Nutanix AOS and Nutanix AHV. Nutanix software is a contracted separately under additional Company ItemIDs. EDGE VDI Only Nodes are licensed only for virtual desktop virtual machines (VMs), and those compute workloads that directly support the virtual desktops. EDGE VDI Only Nodes minimally belong to a Cluster configured with at least three (3) EDGE VDI Only Nodes. EDGE VDI Only Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE VDI Only Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon Gold processors 6342 (2.8 GHz, 24 cores), 48 cores total
- 1024 GB RAM
- Hybrid performance disk configuration consisting of 24TB HDD and 7.68TB SSD
- Two (2) NVIDIA A16 GPU cards installed

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect usable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of EUC and other workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Software Specifications:

- None - contracted separately with additional ItemIDs

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
    - Cluster sizing including heterogeneous Clusters
    - Data tiering
    - Inline compression
    - Inline performance deduplication
    - Online Cluster growth
    - Compression
    - Deduplication
    - Erasure coding (EC-X) *
- Infrastructure Resilience
    - Data path redundancy
    - Tunable redundancy factor

Security
    - Client authentication
    - Cluster lockdown
    - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
    - Prism Central and Prism Elements
    - Pulse
    - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals. Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
    - Virtual Machine (VM) centric snapshots and clones
    - VM-centric Storage QoS
    - VM Flash Mode
- Data Protection
    - Application consistent snapshots
    - Local snapshots
    - Self-service restores
    - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
    - VM management. VM s operating system management and application management is specifically excluded

from this scope.
    - VM automated resource scheduling
    - VM affinity rules
    - Virtual network configuration
    - Host profiles
    - VM high availability
    - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

GPU Administration:

- Manage and maintain NVIDIA Grid Licensing
    - Manage AOS Cluster drivers for NVIDIA grid GPU virtualization software

GPU Triage and Troubleshooting:

- Triage of GPU system incidents
- Troubleshoot and work to resolve GPU system incidents
- Document GPU system issues and errors

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
    - Cluster and VM performance and analysis
    - Cluster and health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection and recovery policies

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Contract for company Nutanix AOS VDI Per VM License Service
- Contract for company NVIDIA Virtual GPU Software services
- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan;

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.
- Client agrees that NVIDIA offerings provided herein are subject to the NVIDIA End User License Agreement for GPU available https://images.nvidia.com/content/pdf/grid/support/enterprise-eula-grid-and-amgx-supplements.pdf which is hereby incorporated into this SOW in full.

603555 ReliaCloud EDGE Reserved Node EUC.4807HGA16-2

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Reserved Node EUC.4807HGA16-2 (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Two (2) Intel Xeon-Gold processors 6342 (2.8 GHz, 24 cores), 48 cores total
- 1024 GB RAM
- Hybrid performance disk configuration consisting of 24TB HDD and 7.68TB SSD
- Two (2) NVIDIA A16 GPU cards installed

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE Activated Reserved Node Rate (separate Itemd ID), until Client submits a service request for a Reserved Node to be:

  A) Removed from the Cluster, at which point the Reserved Node will remain available and billed (commencing the following month) at its Reserved Node rates;

  or

  B) Elevated to production status, at which point the Reserved Node will become part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node EUC.4807HGA16-2 rate (commencing the following month).

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE Node EUC.4807HGA16-2 Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Activated Reserved Node EUC.4807HGA16-2 Services
- Notify Company to request Node activation, deactivation or changes in use to production status

611385 ReliaCloud EDGE Reserved Node EUC.4807HG0

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the

merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Reserved Node EUC.4807HG0 (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Intel processor(s), 48 cores total
- 1536 GB RAM
- Hybrid performance disk configuration consisting of 32TB HDD and 7.68TB NVMe
- GPU capable, zero GPUs installed

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE Activated Reserved Node Rate (separate Itemd ID), until Client submits a service request for a Reserved Node to be:

  A) Removed from the Cluster, at which point the Reserved Node will remain available and billed (commencing the following month) at its Reserved Node rates;

  or

  B) Elevated to production status, at which point the Reserved Node will become part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node EUC.4807HG0 rate (commencing the following month).

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the

Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE Node EUC.4807HG0 Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Activated Reserved Node EUC.4807HG0 Services
- Notify Company to request Node activation, deactivation or changes in use to production status

611386 ReliaCloud EDGE Activated Reserved Node EUC.4807HG0.A

Company's Responsibilities and Included Features

ReliaCloud EDGE Activated Reserved Node EUC.4807HG0.A (Activated Node) service is comprised of hardware, software and a base level of management services for the Nutanix AOS and Nutanix AHV. An Activated Node is a ReliaCloud EDGE Reserved Node EUC.4807HG0 that has been joined to an existing Cluster at Client request and is available for Client s use.

A ReliaCloud EDGE Activated Reserved Node is identical to ReliaCloud EDGE Node EUC.4807HG0.A, except the per Node billing rate as provided above and as otherwise provided within this ItemID. All other Company responsibilities, included features, Client responsibilities and out of scope notes are included as if restated within this ItemID.

Node Activation and Billing

An Activated Node will be billed in whole month increments for each month that it is activated until Client submits a service request for the Activated Node to be:

A) Removed from the Cluster, at which point the Activated Node will be returned to Reserved Node status and rates (commencing the following month);

or

B) Elevated to production status, at which point the Activated Node will become a part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node EUC.4807HG0.A rate (commencing the following month).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Additional General Requirements:

- Subscribe to Company s Services for ReliaCloud EDGE Node EUC.4807HG0.A Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud EDGE Reserved Node EUC.4807HG0 Services

611509 ReliaCloud EDGE Activated Reserved Node EUC.4807HG0.E

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE On-Prem Reserved Node GPC.1630N (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Intel Processor(s), 16 cores total
- 512 GB RAM
- Disk configuration of 30.72TB NVMe

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its monthly ReliaCloud EDGE On-Prem Activated Reserved Node Rate, until Client submits a service request for a Reserved Node to be removed from the Cluster, at which point the Reserved Node will remain available and billed at its Reserved Note rates.

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE On-Prem Node GPC.1630N Services and have a Cluster of at least three (3) Nodes
- Subscribe to Company s ReliaCloud On-Prem EDGE Reserved Activated Node GPC.1630N Services

Notify Company to request Node activation, deactivation or changes in use to production status

611702 ReliaCloud EDGE Reserved Node EUC.4807HGA16-2

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE Reserved Node EUC.4807HGA16-2 (Reserved Node) provides an allocation of compute resources to an existing Cluster of at least 3 Nodes. Upon Client s request, Reserved Nodes are activated from a powered-off state and joined to the Client s existing hosted Cluster.

Node physical specifications

Company will provide a Node that meets or exceeds the following physical specifications:

- Intel processor(s), 48 cores total
- 1536 GB RAM
- Hybrid performance disk configuration consisting of 32TB HDD and 7.68TB NVMe
- Two (2) NVIDIA A16 GPU cards installed

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect useable capacity including but not limited to the Cluster s Node failure resiliency design, storage configurations settings such as deduplication, compression, and encryption, as well as the types of workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Activation and Billing

- Client may request Reserved Node activation at any time by submitting a priority 1 service request
- Reserved Node activation is supported 24 x 7
- A Reserved Node is considered activated once joined to the Cluster and visible within Prism Central
- Once activated the Reserved Node will be billed and serviced under its ReliaCloud EDGE Node EUC.4807HGA16-2 Rate (separate Itemd ID), until Client submits a service request for a Reserved Node to be:

  A) Removed from the Cluster, at which point the Reserved Node will remain available and billed (commencing the following month) at its Reserved Node rates;

  or

  B) Elevated to production status, at which point the Reserved Node will become part of the Cluster for the remaining term of the SOW, billed at the ReliaCloud EDGE Node EUC.4807HGA16-2 rate (commencing the following month).

Service Level Objective (SLO)

- The SLO for Company delivery of a Dedicated Reserved Node to an activated state, from the time of Client request to visibility within Prism Central, is eight (8) Hours. This SLO is subject to the service availability SLA found within the Service Level Agreement Company Services section of this SOW.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Subscribe to Company s ReliaCloud EDGE Node EUC.4807HGA16-2 Services and have a Cluster of at least three (3) Nodes
- Notify Company to request Node activation, deactivation or changes in use to production status

611703 ReliaCloud EDGE EUC.4807HGA16-2.A

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

EUC: End User Compute services also known as Virtual Desktop Infrastructure (VDI), Desktop as a Service (DaaS) and virtual application hosting. EUC is a solution for services which commonly replace the conventional physical desktop with a virtualized platform.

GPU: Graphics processing unit (GPU) is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

ReliaCloud EDGE EUC.4807HGA16-2.A (EDGE VDI Only Node) service is comprised of hardware and a base level of management services for the Nutanix AOS and Nutanix AHV. Nutanix software is a contracted separately under additional Company ItemIDs. EDGE VDI Only Nodes are licensed only for virtual desktop virtual machines (VMs), and those compute workloads that directly support the virtual desktops. EDGE VDI Only Nodes minimally belong to a Cluster configured with at least three (3) EDGE VDI Only Nodes. EDGE VDI Only Nodes are dedicated to the Client for their exclusive use.

Node physical specifications:

Company will provide an EDGE VDI Only Node that meets or exceeds the following physical specifications:

- Intel processor(s), 48 cores total
- 1536 GB RAM
- Hybrid performance disk configuration consisting of 32TB HDD and 7.68TB NVMe
- Two (2) NVIDIA A16 GPU cards installed

Physical specifications are not equivalent to the effective usable capacity of the Node. The effective usable capacity is determined by the overall Cluster configuration. Clusters have a number of configurable parameters that affect usable capacity including but not limited to the Cluster s Node failure resiliency design, storage configuration settings such as deduplication, compression, and encryption, as well as the types of EUC and other workloads and processor over-subscription ratios that run upon the Cluster. Company will consult with Client to determine the appropriate Cluster level settings to meet their business and workload performance goals.

Node Software Specifications:

- None - contracted separately with additional ItemIDs

AOS Administration:

Company will support administration of the following base features of AOS:

- Enterprise storage
  - Cluster sizing including heterogeneous Clusters
  - Data tiering
  - Inline compression
  - Inline performance deduplication
  - Online Cluster growth
  - Compression
  - Deduplication
  - Erasure coding (EC-X) *
- Infrastructure Resilience
  - Data path redundancy
  - Tunable redundancy factor
- Security
  - Client authentication
  - Cluster lockdown
  - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and Analytics
  - Prism Central and Prism Elements
  - Pulse
  - Cluster health

* Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals. Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers.

Cluster and Node Incident Triage and Troubleshooting:

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Block and Node Maintenance Management:

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

AHV Administration:

Company will support administration of the following base features of AHV:

- Enterprise storage
  - Virtual Machine (VM) centric snapshots and clones
  - VM-centric Storage QoS
  - VM Flash Mode
- Data Protection
  - Application consistent snapshots
  - Local snapshots
  - Self-service restores
  - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
  - VM management. VM s operating system management and application management is specifically excluded from this scope.
  - VM automated resource scheduling
  - VM affinity rules
  - Virtual network configuration
  - Host profiles
  - VM high availability
  - Self-service portal

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting:

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

GPU Administration:

- Manage and maintain NVIDIA Grid Licensing
  - Manage AOS Cluster drivers for NVIDIA grid GPU virtualization software

GPU Triage and Troubleshooting:

- Triage of GPU system incidents
- Troubleshoot and work to resolve GPU system incidents
- Document GPU system issues and errors

Co-administration:

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
  - Cluster and VM performance and analysis
  - Cluster and health and availability
  - Cluster capacity and trend info

        - Alerts and notifications
    - Creation of customized dashboards
    - Self-service management of virtual infrastructure
        - Create, delete and modify VMs
        - Execute snapshots and restorations
        - Add VMs to catalog
        - Import, add, create and delete images to catalog
        - Create and modify data protection and recovery policies

Upon Client request Company will provide account(s) with administrator level and or viewer privileges.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Contract for company Nutanix AOS VDI Per VM License Service
- Contract for company NVIDIA Virtual GPU Software services
- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Business Continuity / Disaster Recovery Plan;

- Client is responsible for all disaster recovery solutions and associated services
- Client business continuity plan(s) and disaster recovery plan(s) are Client responsibilities and are out of scope for this engagement.

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.

- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

- Client agrees that NVIDIA offerings provided herein are subject to the NVIDIA End User License Agreement for GPU

available https://images.nvidia.com/content/pdf/grid/support/enterprise-eula-grid-and-amgx-supplements.pdf which is hereby incorporated into this SOW in full.

Family: Data Centers

Category: Accessories

112037 Data Center Access card

Company's Responsibilities and Included Features

- Provide 1 Data center facility proximity badge reader access card identified to a specific user
- Enroll that user into the badge reader security system
- Apply roll based security policies

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Be physically available to receive card at data center location
- User must be an authorized member of the Client's data center access policy

112038 Blanking panel 1RU

Company's Responsibilities and Included Features

- 1U 19" Black Toolless Blanking Panel
- Install Blanking Panel

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

112039 Storage locker 3'x4'x8' (w/d/h)

Company's Responsibilities and Included Features

- Company will provide a storage locker for the purpose of housing IT equipment, or supporting materials such as Media, Cables, Manuals, tools and other accessories
- Storage Locker size is approximately 3' Wide x 4' Deep x 8' Tall
- The locker construction is of wire meshed (caging) materials
- The locker has a digital pin number combo system for security
- No power is provided for the locker
- No SLA is provided around climate controls. Locker spaces are inside the data center, but located outside of the data rooms.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Maintain inventory of the equipment stored in the locker space
- Maintain the security of the PIN number through their organization, or request a PIN code update
- Ensure that the equipment can reside in an environment that is not controlled to Data Center room equipment tolerances
- Store no materials that violate the Data Center Acceptable use policy

112040 Storage locker 4'x5'x8' (w/d/h)

Company's Responsibilities and Included Features

- Company will provide a storage locker for the purpose of housing IT equipment, or supporting materials such as Media,

Cables, Manuals, tools and other accessories.

- Storage Locker size is approximately 4' Wide x 5' Deep x 8' Tall
- The locker construction is of wire meshed (caging) materials
- The locker has a digital pin number combo system for security
- No power is provided for the locker
- No SLA is provided around climate controls. Locker spaces are inside the data center, but located outside of the data rooms.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Maintain inventory of the equipment stored in the locker space
- Maintain the security of the PIN number through their organization, or request a PIN code update
- Ensure that the equipment can reside in an environment that is not controlled to Data Center room equipment tolerances
- Store no materials that violate the Data Center Acceptable use policy

112041 Storage locker 4'x6'x8' (w/d/h)

Company's Responsibilities and Included Features

- Company will provide a storage locker for the purpose of housing IT equipment, or supporting materials such as Media, Cables, Manuals, tools and other accessories.
- Storage Locker size is approximately 4' Wide x 6' Deep x 8' Tall
- The locker construction is of wire meshed (caging) materials
- The locker has a digital pin number combo system for security
- No power is provided for the locker
- No SLA is provided around climate controls. Locker spaces are inside the data center, but located outside of the data rooms.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Maintain inventory of the equipment stored in the locker space
- Maintain the security of the PIN number through their organization, or request a PIN code update
- Ensure that the equipment can reside in an environment that is not controlled to Data Center room equipment tolerances
- Store no materials that violate the Data Center Acceptable use policy

112043 Additional Video Surveillance Camera

Company's Responsibilities and Included Features

- Additional video surveillance Camera for the purpose of providing additional video coverage
- Retain active movement (pixel change detection based) for 180 days
- Per Client request provide a video snippet of the time frame in question
- Maintain/repair/Replace infrastructure as necessary
- Ensure field of view violates no other confidential equipment policy of other Clients
- Install camera and associated network
- Maintain supporting server and storage infrastructure

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Request as necessary video surveillance foot within a specific time frame no greater than 180 days from the date of request.

112044 Cat5e Patch Cable 3'

Company's Responsibilities and Included Features

- Cat 5e Patch Cable:
  - Connectors gender is male, type RJ-45 3' in length

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Install patch cable, label test and certify connectivity

112045 Cat5e Patch Cable 10'

Company's Responsibilities and Included Features

- Cat 5e Patch Cable:
  - Connectors gender is male, type RJ-45 10' in length

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Install patch cable, label test and certify connectivity

112046 1 RU Shelf

Company's Responsibilities and Included Features

- Cabinet shelf with 4 mounting post 1RU height displacement
- EIA-310-D Compliant
- Adjustable mounting Depth, ventilated, max weight 250 lbs
- Install shelf in cabinet

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Load any equipment onto shelf
- Secure equipment to shelf if necessary

112047 Biometric Lock System per Cabinet

Company's Responsibilities and Included Features

- Biometric (fingerprint) lock system with front Biometric reader with key override and back of cabinet electronic integrated reader
- Provide access level reporting details as requested
- Install front and back readers and associated network infrastructure
- Enroll Client's users per request
- Manage and maintain supporting server infrastructure
- Managed and maintain locking mechanisms

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of user additions or deletions
- New users are responsible for arriving on-site for enrollment. Requires fingerprint(s) scanning.

600303 Antenna Space Rental - Rooftop

Company's Responsibilities and Included Features

- Provide rooftop space to accommodate antenna

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide antenna
- Provide antenna mount
- Provide associated antenna cable to reach cabinet

600612 Private Staging Room

Company's Responsibilities and Included Features

- Company will provide a Private Staging Room (staging room) for the purpose of housing IT equipment or supporting materials such as media, cables, manuals, tools and other accessories.
    - The staging room is not designed for dedicated the long-term occupancy of Client support technicians.
    - The staging room is not suitable to run mission-critical infrastructure. It is designed to support the build-up and storage of IT equipment and support materials.
    - Fire suppression controls are water based (overhead sprinkler).
- Staging room size is approximately 20' wide x 24' deep x 18' tall
- The staging room is a secured space, constructed of concrete walls (slab and cinder block), steel doors, and wire-mesh caging materials to partition the space.
- Ingress and egress to the staging room are secured via proximity card access.
- Non-conditioned, non-redundant standard 120v outlets are available.
- The staging room is located inside the data center, but is located outside of the conditioned data rooms.

Service Level Agreement

- No SLA is provided for the availability of power provided to the room.
- No SLA is provided for environmental specifications, for example, temperature and relative humidity.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Maintain inventory of the equipment stored in the locker space
- Provide all staging room furnishings, for example; desks, chairs, counter-top space, shelving, storage bins, lockers, etc.
- Ensure that the equipment can reside in an environment that is not controlled to Data Center data room equipment tolerances
- Store no materials that violate the Data Center Acceptable Use Policy (AUP).
- Contract for colcoation space within the data center facility.

601450

Company's Responsibilities and Included Features

Proximity Card Lock System

- Proximity card locking mechanism, placed on the front and back cabinet doors.
- System integrates with Companies card reader system
- Install front and back readers and associated network infrastructure via separate non-recurring fee.

Management

- Provide access level reporting details as requested.
- Enroll Client's users per request using same proximity card system
- Manage and maintain supporting server infrastructure
- Managed locking mechanisms
- Troubleshooting of system incidents
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues

Provide client with updates
- Document user issues and system errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating system software licensing

- Notify Company of user additions or deletions. \
- New users are responsible for arriving on-site for enrollment.
- Requires part 112037 Data Center Access card (or equivalent) to enroll additional staff beyond initial colocation user allotment.

601971 Storage Locker 36" x 18" x 78"

Company's Responsibilities and Included Features

Storage Locker

- Company will provide a storage locker for the purpose of housing IT equipment, or supporting materials such as media, cables, manuals, tools and other accessories.
- Storage locker size is approximately 36" wide x 18" deep x 78" tall
- The locker construction is metal
- The locker has a key lock.
- No power is provided for the locker
- No SLA is provided around climate controls. Locker spaces are inside the data center, but located outside of the data rooms.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for the following:

- Maintain inventory of the equipment stored in the locker space
- Ensure that the equipment can reside in an environment that is not controlled to Data Center room equipment tolerances
- Store no materials that violate the Data Center Acceptable use policy

603878 Secure Storage Area 4'x2'x6' (w/d/h)

Company's Responsibilities and Included Features(unless covered by another ItemID)

Provide secure storage area in data center outside of data room

Secure Storage Area

- Company will provide a secure storage area for the purpose of housing IT equipment, or supporting materials such as Media, Cables, Manuals, tools and other accessories.
- Secure storage area size is approximately 4' Wide x 2' Deep x 6' Tall
- Secure storage area is behind a card access door only accessible by data center staff
- Access to area available on demand 24X7X365
- No power is provided for the locker
- No SLA is provided around climate controls. Secure area spaces are inside the data center, but located outside of the data rooms.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Secure Storage Area

- Maintain inventory of the equipment stored in the locker space
- Ensure that the equipment can reside in an environment that is not controlled to Data Center room equipment tolerances
- Store no materials that violate the Data Center Acceptable use policy

603932 Secure Room - Lab 142 - 10 X12 (w/d)

Company's Responsibilities and Included Features(unless covered by another ItemID)

Provide secure storage area in data center outside of data room

Secure Storage Area

- Company will provide a secure room (Lab 142) dedicated to Client for the purpose of housing IT equipment, or supporting materials such as Media, Cables, Manuals, tools and other accessories
- Secure room size is approximately 10' Wide x 12' Deep
- Secure room is behind a card access door only accessible by data center staff
- Access to room available on demand 24X7X365
- Power is available in the room for laptops and servers
- No SLA is provided around climate controls. Secure area spaces are inside the data center, but located outside of the data rooms.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Secure Storage Area

- Maintain inventory of the equipment stored in the secure room
- Ensure that the equipment can reside in an environment that is not controlled to Data Center room equipment tolerances
- Store no materials that violate the Data Center Acceptable use policy
- Network access to Client resources in data center
- Additional or customized power

Category: Cabinet Eqv.

112013 Floor Space Equivalent 24" x 48" and 5kW power

Company's Responsibilities and Included Features

The Floor Space Equivalent service is for a Client provided cabinet that is 24" Wide by 48" deep, plus 5 kW (5,000 Watts) of usable power. Company will deliver the following services:

- Usable floor space for the purpose of housing a Client provided cabinet
- Standardized ventilation hood infrastructure (if applicable)
- 5,000 watts (5 kilowatts) of power
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
    - 120v 20a
    - 120v 30a
    - 208v 20a
    - 208v 30a
    - 208v 20a (3-phase)

208v 30a (3-phase)
    - 208v 50a (3-phase)
    - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
    - Equipment power cycling - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's unbadged vendors, employees, and auditors
    - Handling of Client's media (e.g. tapes) including shipping and receiving
    - Provide 24/7 access to data center, and up to 3 access cards per Client.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide an industry approved racking enclosure, 4 sided lockable for the purpose of housing IT infrastructure
- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 5000 watts (5 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.
- Provide Company with access controls to enter the locked enclosure

112014 Floor Space Equivalent 24" x 48" and 10kW power

Company's Responsibilities and Included Features

The Floor Space Equivalent service is for a Client provided cabinet that is 24" Wide by 48" deep, plus 10 kW (10,000 Watts) of usable power. Company will deliver the following services:

- Usable floor space for the purpose of housing a Client provided cabinet
- Standardized ventilation hood infrastructure (if applicable)
- 10,000 watts (10 kilowatts) of power
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
    - 120v 20a
    - 120v 30a
    - 208v 20a
    - 208v 30a
    - 208v 20a (3-phase)
    - 208v 30a (3-phase)
    - 208v 50a (3-phase)
    - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and

rear doors and proper services clearances, and space compliance for height, depth and weight

- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
  - Equipment power cycling
  - Secure patch cable connections
  - Observation of equipment, display indicators and general environment
  - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
  - Escorts of Client's unbadged vendors, employees, and auditors
  - Handling of Client's media (e.g. tapes) including shipping and receiving
  - Provide 24/7 access to data center, and up to 3 access cards per Client.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide an industry approved racking enclosure, 4 sided lockable for the purpose of housing IT infrastructure
- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 10,000 watts (10 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.
- Provide Company with access controls to enter the locked enclosure

500104 Floor Space Equivalent 24" x 48" and 4kW power

Company's Responsibilities and Included Features

The Floor Space Equivalent service is for a Client provided cabinet that is 24" Wide by 48" deep, plus 4 kW (4,000 Watts) of usable power. Company will deliver the following services:

- Usable floor space for the purpose of housing a Client provided cabinet
- Standardized ventilation hood infrastructure (if applicable)
- 4,000 watts (4 kilowatts) of power
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
  - 120v 20a
  - 120v 30a
  - 208v 20a
  - 208v 30a
  - 208v 20a (3-phase)
  - 208v 30a (3-phase)
  - 208v 50a (3-phase)
  - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
  - Equipment power cycling

Secure patch cable connections

- Observation of equipment, display indicators and general environment
- Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
- Escorts of Client's unbadged vendors, employees, and auditors
- Handling of Client's media (e.g. tapes) including shipping and receiving
- Provide 24/7 access to data center, and up to 3 access cards per Client.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide an industry approved racking enclosure, 4 sided lockable for the purpose of housing IT infrastructure
- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 4000 watts (4 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.
- Provide Company with access controls to enter the locked enclosure

500141 Colocation Displacement Space 24" x 48"

Company's Responsibilities and Included Features

Company will provide 24 x 48 floor space for the purpose of providing service clearances for non-standard size equipment, or to provide proper ingress or egress space to accommodate cage walls or cage doors.

- Space is to not be occupied with client equipment other than to facilitate the immediate service of the adjacent equipment
- Space shall be used for no other propose other than to provide services clearances.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Ensure clearance of the displacement space to allow for proper service access to client equipment
- Not occupy the space with colocation infrastructure.

500142 5kW Floor Space Equivalent 24"x48" Metered Power 1.6 PUE

Company's Responsibilities and Included Features

- Up to 5 kW of power infrastructure (actual consumption billed separately)
- Equipment cabinet space up to 24" wide by 48" deep. Not to exceed 79" in height
- Multiple Floor space equivalents may be combined together to support Client provided equipment which exceeds the 24"x48" allocation
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
  - 120v 20a
  - 120v 30a
  - 208v 20a
  - 208v 30a
  - 120v 20a (3-phase)
  - 208v 20a (3-phase)
  - 208v 30a (3-phase)

        - 208v 50a (3-phase)
        - 208v 60a (3-phase)
    - Notification to Client if power maximums are exceeded
    - Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper service clearances, and space compliance for height, depth and weight
    - Provide two (2) hours of remote hands services per Client per month, tracked in 15-minute increments. Remote hands services include:
        - Equipment power cycling
        - Secure patch cable connections
        - Observation of equipment, display indicators and general environment
        - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
        - Escorts of Client's unbadged vendors, employees, and auditors
        - Handling of Client's media (e.g. tapes) including shipping and receiving
    - Provide 24/7 access to data center, and up to 3 access cards per Client. Power Consumption:
        - All pricing is net of utility power consumption, which will be billed monthly based on usage. Utility Consumption Example:
            - Utility consumption will be billed on monthly, metered usage basis using the following formula:
                - Total kW hours consumed x data center PUE x current utility rate. Data Center PUE refers to the Power Utilization Effectiveness ratio, an industry standard measurement of the efficiency of a data center. It is defined as the ratio of the total amount of power used by the data center facility to the power delivered to IT equipment. To demonstrate our commitment to providing an energy efficient facility and passing the savings to our clients, Company will commit to calculating the utility consumption invoice based on a guaranteed data center PUE of 1.6.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide proper colocation infrastructure to accommodate IT infrastructure
- Provide manufacture's specifications for power delivery, ventilation, service clearances, and device security
- Validate with manufacture proper installation to ensure compliance with equipment warranty
- Provide a secondary copy of physical keyed infrastructure to Company for the purpose of emergency support
- Provide all in-rack IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 5 kW
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

606636 Floor Space 30" x 48" up to 17.3kW power

The Floor Space service is for a Client provided cabinet that is 30" Wide by 48" deep, plus up to 20 kW (20,000 Watts) of usable power.

Company's Responsibilities and Included Features

Company will deliver the following services:

- Usable floor space for the purpose of housing a Client provided cabinet
- Requires customized ventilation solution
- Up to 20,000 watts (20 kilowatts) of power
- Power delivered to each Client cabinet via primary and redundant branch circuits requires custom power deliery with

up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
    - 120v 20a
    - 120v 30a
    - 208v 20a
    - 208v 30a
    - 208v 20a (3-phase)
    - 208v 30a (3-phase)
    - 208v 50a (3-phase)
    - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors), proper services clearances, and space compliance for height, depth and weight
- Provide two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's unbadged vendors, employees, and auditors
    - Handling of Client's media (e.g. tapes), including shipping and receiving
    - Provide 24/7 access to data center, and up to 3 access cards per Client

Power Pricing Adjustment

- Company reserves the right to change pricing of this ItemID to reflect rate changes by utility providers

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide an industry approved racking enclosure, 4 sided lockable for the purpose of housing IT infrastructure
- Provide all in-rack IT infrastructure
- Rack and cable the equipment
- Provide customized power solution with circuit and plug type as required by the manufacture's specifications
- Provide customized ventilation solution
- Utilize no more power than the maximum average power density as specified 15,000 watts (15 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.
- Provide Company with access controls to enter the locked enclosure

Category: Cabinet Metered

500115 5kw Metered Cabinet - 1.2 PUE

Company's Responsibilities and Included Features

- 1 Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure
- 5kW of power infrastructure (actual consumption billed separately)
- A single cabinet 24" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of vertical equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
    - 120v 20a
    - 120v 30a
    - 208v 20a

- 208v 30a
- 120v 20a (3-phase)
- 208v 20a (3-phase)
- 208v 30a (3-phase)
- 208v 50a (3-phase)
- 208v 60a (3-phase)

- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper service clearances, and space compliance for height, depth and weight
- Provide two (2) hours of remote hands services per Client per month, tracked in 15-minute increments.

500116 10kw Metered Cabinet - 1.2 PUE

Company's Responsibilities and Included Features

- 1 Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure
- 10 kW of power infrastructure (actual consumption billed separately)
- A single cabinet 24" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of vertical equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
  - 120v 20a
  - 120v 30a
  - 208v 20a
  - 208v 30a
  - 120v 20a (3-phase)
  - 208v 20a (3-phase)
  - 208v 30a (3-phase)
  - 208v 50a (3-phase)
  - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper service clearances, and space compliance for height, depth and weight
- Provide two (2) hours of remote hands services per Client per month, tracked in 15-minute increments. Remote hands services include:
  - Equipment power cycling
  - Secure patch cable connections
  - Observation of equipment, display indicators and general environment
  - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
  - Escorts of Client's unbadged vendors, employees, and auditors
  - Handling of Client's media (e.g. tapes) including shipping and receiving
  - Provide 24/7 access to data center, and up to 3 access cards per Client. Power Consumption: All pricing is net of utility power consumption, which will be billed monthly based on usage. Utility Consumption Example:
    - Utility consumption will be billed on monthly, metered usage basis using the following formula:
      - Total kW hours consumed x data center PUE x current utility rate. Data Center PUE refers to the Power Utilization Effectiveness ratio, an industry standard measurement of the efficiency of a

data center. It is defined as the ratio of the total amount of power used by the data center facility to the power delivered to IT equipment. To demonstrate our commitment to providing an energy efficient facility and passing the savings to our clients, Company will commit to calculating the utility consumption invoice based on a guaranteed data center PUE of 1.2.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in-rack IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 10 kW
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

500152 4kW Metered Cabinet - 1.5 PUE

Company's Responsibilities and Included Features

- 1 Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure
- 4 kW of power infrastructure (actual consumption billed separately)
- A single cabinet 24" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of vertical equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
    - 120v 20a
    - 120v 30a
    - 208v 20a
    - 208v 30a
    - 120v 20a (3-phase)
    - 208v 20a (3-phase)
    - 208v 30a (3-phase)
    - 208v 50a (3-phase)
    - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper service clearances, and space compliance for height, depth and weight
- Provide two (2) hours of remote hands services per Client per month, tracked in 15-minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's unbadged vendors, employees, and auditors
    - Handling of Client's media (e.g. tapes) including shipping and receiving
    - Provide 24/7 access to data center, and up to 3 access cards per Client. Power Consumption:
        - All pricing is net of utility power consumption, which will be billed monthly based on usage. Utility Consumption Example:

Utility consumption will be billed on monthly, metered usage basis using the following formula:

- Total kW hours consumed x data center PUE x current utility rate. Data Center PUE refers to the Power Utilization Effectiveness ratio, an industry standard measurement of the efficiency of a data center. It is defined as the ratio of the total amount of power used by the data center facility to the power delivered to IT equipment. To demonstrate our commitment to providing an energy efficient facility and passing the savings to our clients, Company will commit to calculating the utility consumption invoice based on a guaranteed data center PUE of 1.5.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in-rack IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 4 kW
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

500153 5kW Metered Cabinet - 1.5 PUE

Company's Responsibilities and Included Features

- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper service clearances, and space compliance for height, depth and weight.
- Provide two (2) hours of remote hands services per Client per month, tracked in 15-minute increments. Remote hands services include:
  - Equipment power cycling
  - Secure patch cable connections
  - Observation of equipment, display indicators and general environment
  - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
  - Escorts of Client's unbadged vendors, employees, and auditors
  - Handling of Client's media (e.g. tapes) including shipping and receiving
  - Provide 24/7 access to data center, and up to 3 access cards per Client.
- Power Consumption:
  - All pricing is net of utility power consumption, which will be billed monthly based on usage. Utility Consumption Example:
  - Utility consumption will be billed on monthly, metered usage basis using the following formula:
  - Total kW hours consumed x data center PUE x current utility rate. Data Center PUE refers to the Power Utilization Effectiveness ratio, an industry standard measurement of the efficiency of a data center. It is defined as the ratio of the total amount of power used by the data center facility to the power delivered to IT equipment.
- To demonstrate our commitment to providing an energy efficient facility and passing the savings to our clients, Company will commit to calculating the utility consumption invoice based on a guaranteed data center PUE of 1.5.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in-rack IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 5 kW
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

500154 10kW Metered Cabinet - 1.5 PUE

Company's Responsibilities and Included Features

- 1 Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure
- 10 kW of power infrastructure (actual consumption billed separately)
- A single cabinet 24" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of vertical equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
    - 120v 20a
    - 120v 30a
    - 208v 20a
    - 208v 30a
    - 120v 20a (3-phase)
    - 208v 20a (3-phase)
    - 208v 30a (3-phase)
    - 208v 50a (3-phase)
    - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper service clearances, and space compliance for height, depth and weight
- Provide two (2) hours of remote hands services per Client per month, tracked in 15-minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's unbadged vendors, employees, and auditors - Handling of Client's media (e.g. tapes) including shipping and receiving
    - Provide 24/7 access to data center, and up to 3 access cards per Client. Power Consumption:
        - All pricing is net of utility power consumption, which will be billed monthly based on usage. Utility Consumption Example:
            - Utility consumption will be billed on monthly, metered usage basis using the following formula:
                - Total kW hours consumed x data center PUE x current utility rate. Data Center PUE refers to the Power Utilization Effectiveness ratio, an industry standard measurement of the efficiency of a data center. It is defined as the ratio of the total amount of power used by the data center facility to the power delivered to IT equipment. To demonstrate our commitment to providing an energy efficient facility and passing the savings to our

clients, Company will commit to calculating the utility consumption invoice based on a guaranteed data center PUE of 1.5.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in-rack IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 10 kW
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

500155 15kW Metered Cabinet - 1.5 PUE

Company's Responsibilities and Included Features

- 1 Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure - 15kW of power infrastructure (actual consumption billed separately)
- A single cabinet 24" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of vertical equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
    - 120v 20a
    - 120v 30a
    - 208v 20a
    - 208v 30a
    - 120v 20a (3-phase)
    - 208v 20a (3-phase)
    - 208v 30a (3-phase)
    - 208v 50a (3-phase)
    - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper service clearances, and space compliance for height, depth and weight
- Provide two (2) hours of remote hands services per Client per month, tracked in 15-minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's unbadged vendors, employees, and auditors - Handling of Client's media (e.g. tapes) including shipping and receiving
    - Provide 24/7 access to data center, and up to 3 access cards per Client. Power Consumption:
        - All pricing is net of utility power consumption, which will be billed monthly based on usage. Utility Consumption Example:
            - Utility consumption will be billed on monthly, metered usage basis using the following formula:
                - Total kW hours consumed x data center PUE x current utility rate. Data Center PUE refers to the Power Utilization Effectiveness ratio, an industry standard measurement of

the efficiency of a data center. It is defined as the ratio of the total amount of power used by the data center facility to the power delivered to IT equipment. To demonstrate our commitment to providing an energy efficient facility and passing the savings to our clients, Company will commit to calculating the utility consumption invoice based on a guaranteed data center PUE of 1.5.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in-rack IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 15 kW
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

600572 8kW Metered Cabinet - 1.5 PUE

Company's Responsibilities and Included Features

- 1 Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure
- 8 kW of power infrastructure (actual consumption billed separately)
- A single cabinet 24" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of vertical equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver primary and redundant branch circuit pairs to cabinet
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper service clearances, and space compliance for height, depth and weight
- Provide two (2) hours of remote hands services per Client per month, tracked in 15-minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's unbadged vendors, employees, and auditors
    - Handling of Client's media (e.g. tapes) including shipping and receiving
    - Provide 24/7 access to data center, and up to 3 access cards per Client. Power Consumption:
        - All pricing is net of utility power consumption, which will be billed monthly based on usage. Utility Consumption Example:
            - Utility consumption will be billed on monthly, metered usage basis using the following formula:
            - Total kW hours consumed x data center PUE x current utility rate. Data Center PUE refers to the Power Utilization Effectiveness ratio, an industry standard measurement of the efficiency of a data center. It is defined as the ratio of the total amount of power used by the data center facility to the power delivered to IT equipment. To demonstrate our commitment to providing an energy efficient facility and passing the savings to our clients, Company will commit to calculating the utility consumption invoice based on a guaranteed data center PUE of 1.5.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in-rack IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 8 kW
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

604427 Metered Power DEN 1.2 PUE

Any quantity and price contracted for this ItemID is an estimate only. Actual billing of the ItemId will be based on metered usage and utility price.

604428 Metered Power DEN 1.5 PUE

Any quantity and price contracted for this ItemID is an estimate only. Actual billing of the ItemId will be based on metered usage and utility price.

604430 Metered Power DSM 1.0 PUE

Any quantity and price contracted for this ItemID is an estimate only. Actual billing of the ItemId will be based on metered usage and utility price.

604432 Metered Power DSM 1.5 PUE

Any quantity and price contracted for this ItemID is an estimate only. Actual billing of the ItemId will be based on metered usage and utility price.

604433 Metered Power DSM 1.6 PUE

Any quantity and price contracted for this ItemID is an estimate only. Actual billing of the ItemId will be based on metered usage and utility price.

604435 Metered Power EDP 1.2 PUE

Any quantity and price contracted for this ItemID is an estimate only. Actual billing of the ItemId will be based on metered usage and utility price.

604436 Metered Power EDP 1.5 PUE

Any quantity and price contracted for this ItemID is an estimate only. Actual billing of the ItemId will be based on metered usage and utility price.

604437 Metered Power EDP 1.6 PUE

Any quantity and price contracted for this ItemID is an estimate only. Actual billing of the ItemId will be based on metered usage and utility price.

604439 Metered Power MSN 1.2 PUE

Any quantity and price contracted for this ItemID is an estimate only. Actual billing of the ItemId will be based on metered usage and utility price.

604440 Metered Power MSN 1.5 PUE

Any quantity and price contracted for this ItemID is an estimate only. Actual billing of the ItemId will be based on metered usage and utility price.

604441 Metered Power MSN 1.6 PUE

Any quantity and price contracted for this ItemID is an estimate only. Actual billing of the ItemId will be based on metered usage and utility price.

604444 Metered Power BND 1.5 PUE

Any quantity and price contracted for this ItemID is an estimate only. Actual billing of the ItemId will be based on metered usage and utility price.

606779 5kW Metered Cabinet - 1.0 PUE

Company's Responsibilities and Included Features

- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper service clearances, and space compliance for height, depth and weight.
- Provide six (6) hours of remote hands services per Client per month, tracked in 15-minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's unbadged vendors, employees, and auditors
    - Handling of Client's media (e.g. tapes) including shipping and receiving
    - Provide 24/7 access to data center, and up to 3 access cards per Client.
- Power Consumption:
    - All pricing is net of utility power consumption, which will be billed monthly based on usage. Utility Consumption Example:
    - Utility consumption will be billed on monthly, metered usage basis using the following formula:
    - Total kW hours consumed x data center PUE x current utility rate. Data Center PUE refers to the Power Utilization Effectiveness ratio, an industry standard measurement of the efficiency of a data center. It is defined as the ratio of the total amount of power used by the data center facility to the power delivered to IT equipment.
- To demonstrate our commitment to providing an energy efficient facility and passing the savings to our clients, Company will commit to calculating the utility consumption invoice based on a guaranteed data center PUE of 1.0.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in-rack IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 5 kW

- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

Category: Cabinets

112002 Colocation 2.5kW power and 42RU cabinet -42" deep.

Company's Responsibilities and Included Features

The colocation cabinet service provides a full locking cabinet 24" Wide by 42" deep 42RU high, plus 2.5kW (2,500 Watts) of usable power. Company will deliver the following services:

- One - Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure (if applicable)
- 2,500 watts (2.5 kilowatts) of power
- A single cabinet 24" wide by 42" deep. Each cabinet is 42RU in height. 1RU = 1.75 inches of equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
  - 120v 20a
  - 120v 30a
  - 208v 20a
  - 208v 30a
  - 208v 20a (3-phase)
  - 208v 30a (3-phase)
  - 208v 50a (3-phase)
  - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
  - Equipment power cycling
  - Secure patch cable connections
  - Observation of equipment, display indicators and general environment
  - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
  - Escorts of Client's unbadged vendors, employees, and auditors
  - Handling of Client's media (e.g. tapes) including shipping and receiving
  - Provide 24/7 access to data center, and up to 3 access cards per Client.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 2500 watts (2.5kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

112005 Colocation 2.5kW power and 22RU Half-cabinet

Company's Responsibilities and Included Features

The colocation half-cabinet service provides 22 RU (upper or lower) half of a full-sized locking cabinet (24" Wide by 48" deep) plus 2.5kW (2,500 Watts) of usable power. Company will deliver the following services:

- One - Four sided split height locking enclosure for the purpose of housing IT infrastructure - Locking front and back 1/2 cabinets doors
- Secured middle of rack separation
- Standardized ventilation hood infrastructure (if applicable)
- 2,500 watts (2.5 kilowatts) of power
- A single cabinet 24"" wide by 42"" deep. Each cabinet is 22RU in height. 1RU = 1.75 inches of equipment space
- Mounting rail width is 19""
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to primary and redundant branch circuit pairs per cabinet of the following circuit type:
  - 208v 20a
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
  - Equipment power cycling
  - Secure patch cable connections
  - Observation of equipment, display indicators and general environment
  - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
  - Escorts of Client's unbadged vendors, employees, and auditors
  - Handling of Client's media (e.g. tapes) including shipping and receiving
  - Provide 24/7 access to data center, and up to 3 access cards per Client

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 2500 watts (2.5kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

112006 Colocation 5kW power and 45RU cabinet bundled

Company's Responsibilities and Included Features

The colocation cabinet service provides a full locking cabinet 24" Wide by 48" deep 45RU high, plus 5kW (5000 Watts) of usable power. Company will deliver the following services:

- One - Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure (if applicable)
- 5000 watts (5 kilowatts) of power

- A single cabinet 24" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
    - 120v 20a
    - 120v 30a
    - 208v 20a
    - 208v 30a
    - 208v 20a (3-phase)
    - 208v 30a (3-phase)
    - 208v 50a (3-phase)
    - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's unbadged vendors, employees, and auditors
    - Handling of Client's media (e.g. tapes) including shipping and receiving
    - Provide 24/7 access to data center, and up to 3 access cards per Client

Power Pricing Adjustment

- Company reserves the right to change pricing of this ItemID to reflect rate changes by utility providers

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 5000 watts (5kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

112007 Colocation 10kW power and 45RU cabinet bundled

Company's Responsibilities and Included Features

The colocation cabinet service provides a full locking cabinet 24" Wide by 48" deep 45RU high, plus 10 kW (10,000 Watts) of usable power. Company will deliver the following services:

- One - Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure (if applicable)
- 10,000 watts (10 kilowatts) of power
- A single cabinet 24" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of equipment space
- Mounting rail width is 19"

- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
    - 120v 20a
    - 120v 30a
    - 208v 20a
    - 208v 30a
    - 208v 20a (3-phase)
    - 208v 30a (3-phase)
    - 208v 50a (3-phase)
    - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's unbadged vendors, employees, and auditors
    - Handling of Client's media (e.g. tapes) including shipping and receiving
    - Provide 24/7 access to data center, and up to 3 access cards per Client

Power Pricing Adjustment

- Company reserves the right to change pricing of this ItemID to reflect rate changes by utility providers

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 10,000 watts (10kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

112008 Colocation 15kW power and 45RU cabinet

Company's Responsibilities and Included Features

The colocation cabinet service provides a full locking cabinet 24" Wide by 48" deep 45RU high, plus 15kW (15,000 Watts) of usable power. Company will deliver the following services:

- One - Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure (if applicable) - 15,000 watts (15 kilowatts) of power
- A single cabinet 24" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits.
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
    - 120v 20a

        - 120v 30a
        - 208v 20a
        - 208v 30a
        - 208v 20a (3-phase)
        - 208v 30a (3-phase)
        - 208v 50a (3-phase)
        - 208v 60a (3-phase)
    - Notification to Client if power maximums are exceeded
    - Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
    - Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
        - Equipment power cycling
        - Secure patch cable connections
        - Observation of equipment, display indicators and general environment
        - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
        - Escorts of Client's unbadged vendors, employees, and auditors
        - Handling of Client's media (e.g. tapes) including shipping and receiving
        - Provide 24/7 access to data center, and up to 3 access cards per Client

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 15,000 watts (15 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

112034 Reservation Cabinet for 5kW Power

Company's Responsibilities and Included Features

- Company will reserve the floor space and power of 5 kW for the Client for a period of 12 months from contract signature
- Client may occupy reservation cabinet at any point during the reservation period with two weeks notice
- The reservation service may not be ordered without at least 1 standard (non-reservation) cabinet
- Once the reservation cabinet is occupied it will become subject to standard cabinets rates for the power specified for the duration of services agreement signed for the non-reservation services
- The standard cabinet set up charge will be applied at time of activation
- Client may terminate this reservation option at any point up to 12 months from signature
- Reservation maximum is 12 months from contract signature
- If the reservation cabinet is unoccupied at the end of the reservation maximum, Company reserves the right to return the cabinet to general availability status and may contract the cabinet to another Client or utilize it for another purpose.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company at least two weeks (14 days) prior to taking occupancy of cabinet
- Take occupancy of cabinet before then end of 12 months, or terminate reservation at the end of the reservation period

- Plan for use of the space not to exceed 5 kW

500102 Colocation 4kW power and 48RU cabinet

Company's Responsibilities and Included Features

The colocation cabinet service provides a full locking cabinet 24" Wide by 48" deep 48RU high, plus 4 kW (4000 Watts) of usable power. Company will deliver the following services:

- 1 Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure (if applicable)
- 4000 watts (4 kilowatts) of power
- A single cabinet 24" wide by 48" deep. Each cabinet is 48RU in height. 1RU = 1.75 inches of equipment space.
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
  - 120v 20a
  - 120v 30a
  - 208v 20a
  - 208v 30a
  - 208v 20a (3-phase)
  - 208v 30a (3-phase)
  - 208v 50a (3-phase)
  - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
  - Equipment power cycling
  - Secure patch cable connections
  - Observation of equipment, display indicators and general environment
  - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
  - Escorts of Client's unbadged vendors, employees, and auditors
  - Handling of Client's media (e.g. tapes) including shipping and receiving
- Provide 24/7 access to data center, and up to 3 access cards per Client.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 4000 watts (4 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

500103 Colocation 2kW power and 24RU Half-cabinet

Company's Responsibilities and Included Features

The colocation half-cabinet service provides 24 RU (upper or lower) half of a full-sized locking cabinet (24" Wide by 48" deep) plus 2 kW (2,000 Watts) of usable power. Company will deliver the following services:

- 1 Four sided split height locking enclosure for the purpose of housing IT infrastructure

Locking front and back 1/2 cabinets doors

- Secured middle of rack separation
- Standardized ventilation hood infrastructure (if applicable)
- 2,000 watts (2.0 kilowatts) of power
- A single cabinet 24"" wide by 42"" deep. Each cabinet is 24RU in height. 1RU = 1.75 inches of equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to primary and redundant branch circuit pairs per cabinet of the following circuit type:
  - 208v 20a
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
  - Equipment power cycling
  - Secure patch cable connections
  - Observation of equipment, display indicators and general environment
  - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
  - Escorts of Client's unbadged vendors, employees, and auditors
  - Handling of Client's media (e.g. tapes) including shipping and receiving
  - Provide 24/7 access to data center, and up to 3 access cards per Client

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 2000 watts (2.0 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

500105 Reservation Cabinet for 4kW Power

Company's Responsibilities and Included Features

- Company will reserve the floor space and power of 4 kW for the Client for a period of 12 months from contract signature
- Client may occupy reservation cabinet at any point during the reservation period with two weeks notice
- The reservation service may not be ordered without at least 1 standard (non-reservation) cabinet
- Once the reservation cabinet is occupied it will become subject to standard cabinets rates for the power specified for the duration of services agreement signed for the non-reservation services
- The standard cabinet set up charge will be applied at time of activation
- Client may terminate this reservation option at any point up to 12 months from signature
- Reservation maximum is 12 months from contract signature
- If the reservation cabinet is unoccupied at the end of the reservation maximum, Company reserves the right to return the cabinet to general availability status and may contract the cabinet to another Client or utilize it for another purpose.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company at least two weeks (14 days) prior to taking occupancy of cabinet
- Take occupancy of cabinet before then end of 12 months, or terminate reservation at the end of the reservation period
- Plan for use of the space not to exceed 4 kW

500113 10kw Metered Cabinet - 1.6 PUE

Company's Responsibilities and Included Features

- 1 Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure
- 10 kW of power infrastructure (actual consumption billed separately)
- A single cabinet 24" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of vertical equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
    - 120v 20a
    - 120v 30a
    - 208v 20a
    - 208v 30a
    - 120v 20a (3-phase)
    - 208v 20a (3-phase)
    - 208v 30a (3-phase)
    - 208v 50a (3-phase)
    - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper service clearances, and space compliance for height, depth and weight
- Provide two (2) hours of remote hands services per Client per month, tracked in 15-minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's unbadged vendors, employees, and auditors
    - Handling of Client's media (e.g. tapes) including shipping and receiving
    - Provide 24/7 access to data center, and up to 3 access cards per Client. Power Consumption: All pricing is net of utility power consumption, which will be billed monthly based on usage. Utility Consumption Example:
        - Utility consumption will be billed on monthly, metered usage basis using the following formula:
            - Total kW hours consumed x data center PUE x current utility rate. Data Center PUE refers to the Power Utilization Effectiveness ratio, an industry standard measurement of the efficiency of a data center. It is defined as the ratio of the total amount of power used by the data center facility to the power delivered to IT equipment. To demonstrate our commitment to providing an energy efficient facility and passing the savings to our clients, Company will commit to calculating the utility consumption invoice based on a guaranteed data center PUE of 1.6.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in-rack IT infrastructure

Rack and cable the equipment

- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 10 kW
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

500157 Carrier Cabinet 3kW

Company's Responsibilities and Included Features

The Carrier Cabinet service provides a dedicated locking cabinet enclosure or floor space equivalent should a Client provided be preferred within one of the Data Center Telecommunication rooms. The Carrier Cabinet includes up to 3 kW of usable power. Telecommunications rooms are secured environments. All access is via Company provided escort only. Client will not be issued direct access room badges. Company will provide the following services:

- 1 Four sided locking enclosure for the purpose of housing IT/Telecommunications infrastructure
- 3 kW of power infrastructure
- Up to 3 kW of power delivery
- A single cabinet measuring at least 24" wide, 30" deep and 40RU in height. 1RU = 1.75 inches of equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver one branch circuit pair per cabinet of the following circuit type options:
  - 120v 20a
  - 120v 30a
  - 208v 20a
  - 208v 30a
  - 120v 20a (3-phase)
  - 208v 20a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper service clearances, and space compliance for height, depth and weight
- Provide two (2) hours of remote hands services per Client per month, tracked in 15-minute increments. Remote hands services include:
  - Equipment power cycling
  - Secure patch cable connections
  - Observation of equipment, display indicators and general environment
  - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
  - Escorts of Client's vendors, employees, and auditors
  - Handling of Client's media (e.g. tapes) including shipping and receiving
  - Provide 24/7 access to data center

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in-rack IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum power density as specified 3 kW
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed

and meet all applicable local and national electric codes.

600324 Colocation 8kW power and 48RU cabinet bundled

Company's Responsibilities and Included Features

The colocation cabinet service provides a full locking cabinet 24" Wide by 48" deep 48RU high, plus 8 kW (8000 Watts) of usable power. Company will deliver the following services:

- 1 Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure (if applicable)
- 8000 watts (8 kilowatts) of power
- A single cabinet 24" wide by 48" deep. Each cabinet is 48RU in height. 1RU = 1.75 inches of equipment space.
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
  - 120v 20a
  - 120v 30a
  - 208v 20a
  - 208v 30a
  - 208v 20a (3-phase)
  - 208v 30a (3-phase)
  - 208v 50a (3-phase)
  - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
-
  - Equipment power cycling
  - Secure patch cable connections
  - Observation of equipment, display indicators and general environment
  - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
  - Escorts of Client's unbadged vendors, employees, and auditors
  - Handling of Client's media (e.g. tapes) including shipping and receiving
- Provide 24/7 access to data center, and up to 3 access cards per Client.

Power Pricing Adjustment

- Company reserves the right to change pricing of this ItemID to reflect rate changes by utility providers

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 8000 watts (8 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed

and meet all applicable local and national electric codes.

600326 Colocation 2.5kW power and 45RU cabinet bundled

Company's Responsibilities and Included Features

The colocation cabinet service provides a full locking cabinet 24" Wide by 48" deep 45RU high, plus 2.5kW (2,500 Watts) of usable power. Company will deliver the following services:

- One-Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure (if applicable)
- 2,500 watts (2.5 kilowatts) of power
- A single cabinet 24" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of equipment space
- Mounting rail width is 19""
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
  - 120v 20a
  - 120v 30a
  - 208v 20a
  - 208v 30a
  - 208v 20a (3-phase)
  - 208v 30a (3-phase)
  - 208v 50a (3-phase)
  - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
  - Equipment power cycling
  - Secure patch cable connections
  - Observation of equipment, display indicators and general environment
  - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
  - Escorts of Client's unbadged vendors, employees, and auditors
  - Handling of Client's media (e.g. tapes) including shipping and receiving
  - Provide 24/7 access to data center, and up to 3 access cards per Client

Power Pricing Adjustment

- Company reserves the right to change pricing of this ItemID to reflect rate changes by utility providers

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 2500 watts (2.5kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

600390 Colocation 2.5kW power and 45RU Cabinet bundled for Managed Environments

Company's Responsibilities and Included Features

The colocation cabinet service provides a full locking cabinet 24" Wide by 48" deep 45RU high, plus 2.5kW (2,500 Watts) of usable power for managed environments. Client will not have direct physical access to the cabinet without escort from Company. Company will deliver the following services:

- One-four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure (if applicable)
- 2,500 watts (2.5 kilowatts) of power
- A single cabinet 24" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
    - 120v 20a
    - 120v 30a
    - 208v 20a
    - 208v 30a
    - 208v 20a (3-phase)
    - 208v 30a (3-phase)
    - 208v 50a (3-phase)
    - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth, and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15-minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hotplug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's unbadged vendors, employees, and auditors
    - Handling of Client's media (e.g. tapes) including shipping and receiving

Power Pricing Adjustment

- Company reserves the right to change pricing of this ItemID to reflect rate changes by utility providers

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all IT infrastructure within cabinet
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 2500 watts (2.5kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.
- Client may elect to provide their own cabinet.
- Client provided cabinets must be UL listed and meet all applicable local and national codes.
- Client provided cabinets must not exceed the standard cabinet foot print of 24" wide by 48" deep and 45 RU high.

600445 Colocation 2.5kW power and 21RU half-cabinet bundled

Company's Responsibilities and Included Features

The colocation half-cabinet metered power service provides 21 RU of equipment space and power infrastructure to support 2.5kW of power consumption. Service includes 2.5kW of power usage. Company will deliver the following services:

Cabinet Compartment

- 21 RU secured cabinet compartment via locking front and back cabinets doors. The compartment also includes top and bottom separating panels.
-
    - 1RU = 1.75 inches of equipment space
- A single cabinet approximately 24" wide by 48" deep
- Standard 19" mounting rails
- Top and bottom cable raceway
- Cabinet divider
- Vertical exhaust ducts

Power

- 2.5 kilowatts of power infrastructure. Power usage up to 2.5kW is included.
- Power delivered to each Client cabinet via primary and redundant branch circuits.
- Delivery of primary and redundant branch circuit pairs to support 2.5kW of power consumption.

Management

- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15-minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hot-plug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's unbadged vendors, employees, and auditors
    - Handling of Client's media (e.g. tapes) including shipping and receiving
    - Provide 24/7 access to data center, and up to 3 access cards per Client

Power Pricing Adjustment

- Company reserves the right to change pricing of this ItemID to reflect rate changes by utility providers

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacturer's specifications
- Utilize no more power than the maximum average power density as specified 2500 watts (2.5kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

600446 Colocation 2.0 kW power and 21RU half-cabinet bundled

Company's Responsibilities and Included Features

The colocation half-cabinet metered power service provides 21 RU of equipment space and power infrastructure to support 2kW of power consumption. Service includes 2kW of power usage. Company will deliver the following services:

Cabinet Compartment

- 21 RU secured cabinet compartment via locking front and back cabinets doors. The compartment also includes top and bottom separating panels.
-
    - 1RU = 1.75 inches of equipment space
- A single cabinet approximately 28" wide by 48" deep
- Standard 19" mounting rails
- Top and bottom cable raceway
- Cabinet divider
- Vertical exhaust ducts

Power

- 2.5 kilowatts of power infrastructure. Power usage up to 2kW is included.
- Power delivered to each Client cabinet via primary and redundant branch circuits.
- Delivery of primary and redundant branch circuit pairs per cabinet of the following circuit type 208v 20a.

Managment

- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hotplug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's unbadged vendors, employees, and auditors
    - Handling of Client's media (e.g. tapes) including shipping and receiving
    - Provide 24/7 access to data center, and up to 3 access cards per Client

Power Pricing Adjustment

- Company reserves the right to change pricing of this ItemID to reflect rate changes by utility providers

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacturer's specifications
- Utilize no more power than the maximum average power density as specified 2000 watts (2kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

600641 Colocation 2kW - Two-Post Carrier Rack

Company's Responsibilities and Included Features

The Two Post Carrier Rack service provides a dedicated two-post rack. The Carrier Cabinet includes up to 2 kW of usable power. Telecommunications areas are restricted access environments. All access is via Company provided escort only.

- 1 (one) two post, free-standing equipment rack. Two post racks, do not contain doors, side panels, locks, or other securing measures.
- Up to 2kW of power delivery
- Provides at least 45RU in height. 1RU = 1.75 inches of equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver one branch circuit pair per rack:120v 20a
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper service clearances, and space compliance for height, depth and weight.
- Provide two (2) hours of remote hands services per Client per month, tracked in 15-minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's vendors, employees, and auditors
    - Handling of Client's media (e.g. tapes) including shipping and receiving
    - Provide 24/7 access to data center

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all IT infrastructure within the rack.
- Rack and cable the equipment.
- Specify the correct circuit and plug type as required by the manufacturer's specifications.
- Utilize no more power than the maximum power density as specified 2 kW.
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric code.

600645 Colocation 1.5kW power and 21RU half-cabinet bundled

Company's Responsibilities and Included Features

The colocation half-cabinet metered power service provides 21 RU of equipment space and power infrastructure to support 1.5kW of power consumption. Service includes 1.5kW of power usage. Company will deliver the following services:

Cabinet Compartment

- 21 RU secured cabinet compartment via locking front and back cabinets doors. The compartment also includes top and bottom separating panels.
-
    - 1RU = 1.75 inches of equipment space
- A single cabinet approximately 24" wide by 48" deep
- Standard 19" mounting rails
- Top and bottom cable raceway
- Cabinet divider
- Vertical exhaust ducts

Power

- 1.5 kilowatts of power infrastructure. Power usage up to 1.5kW is included.
- Power delivered to each Client cabinet via primary and redundant branch circuits.
- Delivery of primary and redundant branch circuit pairs to support 1.5kW of power consumption.

Management

- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15-minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hot-plug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's unbadged vendors, employees, and auditors
    - Handling of Client's media (e.g. tapes) including shipping and receiving
    - Provide 24/7 access to data center, and up to 3 access cards per Client

Power Pricing Adjustment

- Company reserves the right to change pricing of this ItemID to reflect rate changes by utility providers

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacturer's specifications
- Utilize no more power than the maximum average power density as specified 1500 watts (1.5kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

601454

Company's Responsibilities and Included Features

The colocation cabinet service provides a full locking cabinet 24" Wide by 48" deep 45RU high, plus 4 kW (4000 Watts) of usable power. Company will deliver the following services:

- 1 Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure (if applicable)
- 4000 watts (4 kilowatts) of power
- A single cabinet 24" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of equipment space.
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
    - 120v 20a
    - 120v 30a
    - 208v 20a
    - 208v 30a
    - 208v 20a (3-phase)
    - 208v 30a (3-phase)
    - 208v 50a (3-phase)
    - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
- Observation of equipment, display indicators and general environment
- Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
- Escorts of Client's unbadged vendors, employees, and auditors
- Handling of Client's media (e.g. tapes) including shipping and receiving
- Provide 24/7 access to data center, and up to 3 access cards per Client.

Power Pricing Adjustment

- Company reserves the right to change pricing of this ItemID to reflect rate changes by utility providers

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 4000 watts (4 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

601455

Company's Responsibilities and Included Features

The colocation cabinet service provides a full locking cabinet 24" Wide by 48" deep 45RU high, plus 8 kW (8000 Watts) of usable power. Company will deliver the following services:

- 1 Four sided locking enclosure for the purpose of housing IT infrastructure

- Standardized ventilation hood infrastructure (if applicable)
- 8000 watts (8 kilowatts) of power
- A single cabinet 24" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of equipment space.
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver up to 3 primary and redundant branch circuit pairs per cabinet of the following circuit type options:
    - 120v 20a
    - 120v 30a
    - 208v 20a
    - 208v 30a
    - 208v 20a (3-phase)
    - 208v 30a (3-phase)
    - 208v 50a (3-phase)
    - 208v 60a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
- Observation of equipment, display indicators and general environment
- Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
- Escorts of Client's unbadged vendors, employees, and auditors
- Handling of Client's media (e.g. tapes) including shipping and receiving
- Provide 24/7 access to data center, and up to 3 access cards per Client.

Power Pricing Adjustment

- Company reserves the right to change pricing of this ItemID to reflect rate changes by utility providers

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 8000 watts (8 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

601891 Additional 1 kW for Two-Post Carrier Rack

Company's Responsibilities and Included Features

The Additional 1 kW for Two-Post Carrier Rack service provides incremental usable power for an existing colocation client as follows:

- 1 kW of additional power delivery
- Notification to Client if power maximums are exceeded

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Any applicable one-time charges for additional circuits or PDUs (power distribution unit).
- Utilize no more power than the maximum power density of the overall cabinet.
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

603496 Colocation 15kW Non-redundant power and 45RU cabinet

Company's Responsibilities and Included Features

The colocation cabinet service provides a full locking cabinet 24" Wide by 48" deep 45RU high, plus 15kW (15000 Watts) of usable power. Company will deliver the following services:

- One - Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure (if applicable)
- 15000 watts (15 kilowatts) of power
- A single cabinet 24" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary, non-redundant branch circuits
- Deliver 2 primary non-redundant branch circuits per cabinet of the following circuit type:
  - 208v 30a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
  - Equipment power cycling
  - Secure patch cable connections
  - Observation of equipment, display indicators and general environment
  - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
  - Escorts of Client's unbadged vendors, employees, and auditors
  - Handling of Client's media (e.g. tapes) including shipping and receiving
  - Provide 24/7 access to data center, and up to 3 access cards per Client

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 15000 watts (15kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

603497 Colocation 10kW Non-redundant power and 45RU cabinet

Company's Responsibilities and Included Features

The colocation cabinet service provides a full locking cabinet 24" Wide by 48" deep 45RU high, plus 10kW (10000 Watts) of usable power. Company will deliver the following services:

- One - Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure (if applicable)
- 10000 watts (10 kilowatts) of power
- A single cabinet 24" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary, non-redundant branch circuits
- Deliver 2 primary non-redundant branch circuits per cabinet of the following circuit type:
    - 208v 30a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's unbadged vendors, employees, and auditors
    - Handling of Client's media (e.g. tapes) including shipping and receiving
    - Provide 24/7 access to data center, and up to 3 access cards per Client

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 10000 watts (10kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

603560 Reservation Cabinet for 8kW Power

Company's Responsibilities and Included Features

- Company will reserve the floor space and power of 8 kW for the Client for a period of 12 months from contract signature
- Client may occupy reservation cabinet at any point during the reservation period with two weeks notice
- The reservation service may not be ordered without at least 1 standard (non-reservation) cabinet
- Once the reservation cabinet is occupied it will become subject to standard cabinets rates for the power specified for the duration of services agreement signed for the non-reservation services
- The standard cabinet set up charge will be applied at time of activation
- Client may terminate this reservation option at any point up to 12 months from signature
- Reservation maximum is 12 months from contract signature
- If the reservation cabinet is unoccupied at the end of the reservation maximum, Company reserves the right to return the cabinet to general availability status and may contract the cabinet to another Client or utilize it for another purpose.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company at least two weeks (14 days) prior to taking occupancy of cabinet
- Take occupancy of cabinet before then end of 12 months, or terminate reservation at the end of the reservation period
- Plan for use of the space not to exceed 8 kW

611096 Cabinet Right Of First Refusal

Company grants Client a 5 day Right of First Refusal (ROFR) for the number of cabinets as listed on the SOW or CO. These cabinets will be adjacent to the existing contracted cabinets or the cabinets contracted under this SOW and/or listed by specific cabinet locations in the line item notes of this SOW or CO.

If, during the term of this SOW, Company has another client wishing to contract any or all of the adjacent ROFR cabinets, Company will give Client written notice of Client s ROFR and the number of applicable cabinets subject to the ROFR. Client shall have 5 business days to accept such cabinet(s) by signing a CO or a new SOW for such cabinets. If Client does not sign a CO or a new SOW for the cabinets within said 5 days, Company shall be free to contract such cabinets with its other client, and the ROFR will be removed from the Client s SOW through a CO. If Client accepts the ROFR, the cabinets will be added to Client s SOW through a CO and billing will begin immediately at the Company s then-current pricing for such cabinets.

611670 Colocation 10kW power and 45RU cabinet bundled - 30 Inch Cabinet

Company's Responsibilities and Included Features

The colocation cabinet service provides a full locking cabinet 30" Wide by 48" deep 45RU high, plus 10 kW (10,000 Watts) of usable power. Company will deliver the following services:

- One - Four sided locking enclosure for the purpose of housing IT infrastructure
- Standardized ventilation hood infrastructure (if applicable)
- 10,000 watts (10 kilowatts) of power
- A single cabinet 30" wide by 48" deep. Each cabinet is 45RU in height. 1RU = 1.75 inches of equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper services clearances, and space compliance for height, depth and weight
- Provide Two (2) hours of remote hands services per Client per month, tracked in 15 minute increments. Remote hands services include:
    - Equipment power cycling
    - Secure patch cable connections
    - Observation of equipment, display indicators and general environment
    - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
    - Escorts of Client's unbadged vendors, employees, and auditors
    - Handling of Client's media (e.g. tapes) including shipping and receiving
    - Provide 24/7 access to data center, and up to 3 access cards per Client

Power Pricing Adjustment

- Company reserves the right to change pricing of this ItemID to reflect rate changes by utility providers

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications

- Utilize no more power than the maximum average power density as specified 10,000 watts (10kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

810312 10RU Carrier Cabinet Space 750Watts

Company's Responsibilities and Included Features

The 10 Rack Unit (RU) Carrier Cabinet Space service provides space in a shared locking cabinet within one of the Data Center Telecommunication rooms. The services includes up to 750 Watts of usable power. Telecommunications rooms are secured environments. All access is via Company provided escort only. Client will not be issued direct access room badges. Company will provide the following services:

- 1 Four sided shared (multi-tenant) locking enclosure for the purpose of housing IT/Telecommunications infrastructure
- 750 Watts of power infrastructure
- Up to 750 Watts of power delivery
- Space inside shared cabinet not to exceed 10RU. 1RU = 1.75 inches of equipment space
- Mounting rail width is 19"
- Power delivered to each Client cabinet via primary and redundant branch circuits
- Deliver one branch circuit pair per cabinet of the following circuit type options:
  - 120v 20a
  - 120v 30a
  - 208v 20a
  - 208v 30a
  - 120v 20a (3-phase)
  - 208v 20a (3-phase)
- Notification to Client if power maximums are exceeded
- Validate compliance with applicable codes and zoning ordinances, proper airflow, proper security (locking front and rear doors and proper service clearances, and space compliance for height, depth and weight
- Provide two (2) hours of remote hands services per Client per month, tracked in 15-minute increments. Remote hands services include:
  - Equipment power cycling
  - Secure patch cable connections
  - Observation of equipment, display indicators and general environment
  - Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
  - Escorts of Client's vendors, employees, and auditors
  - Handling of Client's media (e.g. tapes) including shipping and receiving
  - Provide 24/7 access to data center

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in-rack IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum power density as specified 750 Watts
- Utilize no more in cabinet space than 10 RU

Category: Cross Connections

112016 Carrier Cross-Connection: DS0(POTS)/ISDN

Company's Responsibilities and Included Features

The cross connection service delivers a physical connection from the Data Center Telecommunications rooms to the Client demarcation point.

- Single physical cable delivered structured cable plant to the Client demarcation point.
- Demarcation points are either the Client occupied colocation cabinet, or in the ReliaCloud Integration cabinet.
- Single Pair Category 3, Adapter Interface RJ-45
- Support of cable and terminations
- Maintain on-site inventory or replacement materials (cable and connectors)
- Maintenance and protection of cable fiber pathways

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Order and maintain circuit with vendor of choice
- Provide end termination equipment
- Provide circuit identification Numbers

112017 Carrier Cross-Connection: T1 (DS1)

Company's Responsibilities and Included Features

The cross connection service delivers a physical connection from the Data Center Telecommunications rooms to the Client demarcation point.

- Single physical cable delivered structured cable plant to the Client demarcation point
- Demarcation points are either the Client occupied colocation cabinet, or in the ReliaCloud Integration cabinet
- Two Pair Category 3, Adapter Interface RJ-45 - Support of cable and terminations
- Maintain on-site inventory or replacement materials (cable and connectors)
- Maintenance and protection of cable fiber pathways

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Order and maintain circuit with vendor of choice
- Provide end termination equipment
- Provide circuit identification Numbers

112019 Carrier Cross-Connection: OC3

Company's Responsibilities and Included Features

The cross connection service delivers a physical connection from the Data Center Telecommunications rooms to the Client demarcation point.

- Single physical cable delivered structured cable plant to the Client demarcation point. Demarcation points are either the Client occupied colocation cabinet, or in the ReliaCloud Integration cabinet.
- Multimode or Singlemode fiber, Adapter Interface UPC LC
- Support of cable and terminations
- Maintain on-site inventory or replacement materials (cable and connectors)
- Maintenance and protection of cable fiber pathways

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Order and maintain circuit with vendor of choice
- Provide end termination equipment
- Provide circuit identification Numbers
- Specify Multimode or Singlemode fiber

112020 Carrier Cross-Connection: Ethernet

Company's Responsibilities and Included Features

The cross connection service delivers a physical connection from the Data Center Telecommunications rooms to the Client demarcation point.

- Single physical cable delivered structured cable plant to the Client demarcation point. Demarcation points are either the Client occupied colocation cabinet, or in the ReliaCloud Integration cabinet.
- Category 5e, Adapter Interface RJ-45
- Support of cable and terminations
- Maintain on-site inventory or replacement materials (cable and connectors)
- Maintenance and protection of cable fiber pathways

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Order and maintain circuit with vendor of choice
- Provide end termination equipment
- Provide circuit identification Numbers

112021 Carrier Cross-Connection: Fiber Optic Cross-Connect

Company's Responsibilities and Included Features

The cross connection service delivers a physical connection from the Data Center Telecommunications rooms to the Client demarcation point.

- Single physical cable delivered structured cable plant to the Client demarcation point. Demarcation points are either the Client occupied colocation cabinet, or in the ReliaCloud Integration cabinet.
- Singlemode Fiber, UPC/LC
- Support of cable and terminations
- Maintain on-site inventory or replacement materials (cable and connectors)
- Maintenance and protection of cable fiber pathways

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Order and maintain circuit with vendor of choice
- Provide end termination equipment
- Provide circuit identification Numbers

112022 Carrier Cross-Connection: Coax Cable TV

Company's Responsibilities and Included Features

The cross connection service delivers a physical connection from the Data Center Telecommunications rooms to the Client demarcation point.

- Single physical cable delivered structured cable plant to the Client demarcation point. Demarcation points are either the Client occupied colocation cabinet, or in the ReliaCloud Integration cabinet.
- CATV grade Coax (RG) Adapter Interface F Connector Bulkhead
- Support of cable and terminations
- Maintain on-site inventory or replacement materials (cable and connectors)
- Maintenance and protection of cable fiber pathways

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Order and maintain circuit with vendor of choice
- Provide end termination equipment
- Provide circuit identification Numbers

601762 Use of Network Fiber Ducting

Company's Responsibilities and Included Features

This Service provides for the use of Company fiber ducting into the Company data center to the data center telecommunications rooms, to the Client cabinet as follows:

- Use is limited to a single physical fiber cable
- Escorted Client access to data center telecommunications rooms during installation only
- No cable termination allowed in the data center telecommunications room
- Company provided maintenance and protection of cable fiber ducting

Client's Responsibilities and Out-of-Scope Notes

- Termination of cable required at Client s cabinet
- Client is responsible for providing all equipment and supplies
- Client is responsible for laying fiber cable to Client s cabinet
- Company oversight of laying of fiber cable is required

604666 Enterprise Cross-Connect

Company s Responsibilities and Included Features

General

Enterprise Cross-Connect delivers a managed, documented and secured physical connection from the Data Center Telecommunications rooms to the Client demarcation point.

- Single physical cable delivered via Company s structured cabling plant to the Client demarcation point
- Demarcation points are either the Client contracted colocation cabinet, or in the ReliaCloud Integration cabinet
- Supported media and connector types
  - CAT3
  - CAT5
  - CAT5E
  - CAT6
  - Fiber optic (single-mode or multi-mode)
  - Coaxial cable
- Support of cable and terminations
- Maintain on-site inventory of replacement materials (cables and connectors)
- Maintenance and protection of cable fiber pathways
- Up-to-date documentation in Client-specific Company Configuration Management Database (CMDB)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another Item ID)

- Work with carrier to complete cross connect requirements form (provided separately by Company)
- Order and maintain circuit with vendor of choice
- Provide end termination equipment
- Provide circuit identification numbers

611722 Use of Network Fiber Ducting

Company's Responsibilities and Included Features

This Service provides for the use of Company fiber ducting into the Company data center to the data center telecommunications rooms, to the Client cabinet as follows:

- Use is limited to a single physical nonmetallic innerduct containing multiple pairs of fiber of no more than .75 diameter
- Escorted Client access to data center telecommunications rooms during installation only
- No cable termination allowed in the data center telecommunications room
- Company provided maintenance and protection of cable fiber ducting

Client's Responsibilities and Out-of-Scope Notes

- Termination of cable required at Client's cabinet
- Client is responsible for providing all equipment and supplies
- Client is responsible for bringing fiber cable into the data center
- Company oversight of laying of fiber cable is required

Category: Internet

110003 Colocation Internet Committed - 1Gb

Company's Responsibilities and Included Features

Company will provide a redundant, multi-provider, managed Internet Bandwidth to provide high performance, highly available Internet access. Company will load balance traffic over multiple upstream Internet backbone providers.

- Service may be capped up to the maximum allocation size indicated on the service order.
- Service may also leverage Colocation Burstable Internet bandwidth ItemID 110004, calculated on the 95% of peak usage
- Deliver committed Internet bandwidth allocation in 1 Mbps increments
- Maximum port speed of 1Gbps
- Deliver services via Ethernet on 2 RJ-45 CAT5e or CAT6 links from redundant Internet delivery switches
- Provide a base allocation of up to 3 usable via (/29 network) Internet routing IPv4 Public addresses, unless the Client provides their own ASN and IPv4 portable address space
- Provide access to upstream and downstream bandwidth usage graphs via Client portal

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Comply with acceptable use policy
- Provide termination hardware for service. Requires RJ-45 Ethernet termination ports.
- Notify Company if additional bandwidth is needed beyond the committed allocation
- Commit to at least 1 Mbps of Committed Internet bandwidth

110004 Colocation Internet Burstable - 1Gb

Company's Responsibilities and Included Features

The Colocation Internet Burstable Service is add-on component to Item ID 110003 Colocation Internet Committed Service.

- Clients will have a maximum burst capacity of 1 Gbps.
- Bandwidth utilization in excess of the Committed Bandwidth will be billed as Burstable Bandwidth and calculated using the 95th Percentile Method, in 1 Mbps increments.

The 95th Percentile Method involves polling both inbound and outbound bandwidth utilization every five (5) minutes during each calendar month. All such samples are ordered from highest to lowest. The top 5 percent of readings are discarded, and Client is billed an additional charge based on the next highest reading. The amount of pre-purchased Committed Bandwidth is subtracted from the 95th Percentile to determine the Burstable Bandwidth usage to be billed. Committed Bandwidth is billed in advance; Burstable Bandwidth is billed in arrears, the month after usage occurs. By requesting a hard limit higher than the Committed Bandwidth, Client agrees to be subject to the Burstable Bandwidth for bandwidth consumed beyond the Committed Bandwidth rate level on a monthly basis.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Comply with Internet acceptable use policy
- Commit to at least 1 Mbps of Colocation Internet Committed bandwidth ItemID 110003

600438 Internet IP Address Range for Colocation /24 (256 addresses)

Company's Responsibilities and Included Features

- Provide an Internet routable IPv4 subnet /24 address range
- The address range provides 256 subnet addresses. Note that usable address space within that subnet will vary depending on network routing schema and Client terminating equipment.
- Maintain Internet routing tables
- Maintain all IP documentation
- Enforce IP conservation policies
- Company reserves the right to reclaim any unused address space or space that is not supplied with proper ARIN documentation.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide justification documentation for IP compliance requirements from the American Registry for Internet Numbers (ARIN).
- Stay within ARIN's usage compliance requirements
- Provide network end termination equipment within the Client environment

600439 Internet IP Address Range for Colocation /25 (128 addresses)

Company's Responsibilities and Included Features

- Provide an Internet routable IPv4 subnet /25 address range
- The address range provides 128 subnet addresses. Note that usable address space within that subnet will vary depending on network routing schema and Client terminating equipment.
- Maintain Internet routing tables
- Maintain all IP documentation
- Enforce IP conservation policies
- Company reserves the right to reclaim any unused address space or space that is not supplied with proper ARIN documentation.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide justification documentation for IP compliance requirements from the American Registry for Internet Numbers (ARIN).
- Stay within ARIN's usage compliance requirements
- Provide network end termination equipment within the Client environment

600440 Internet IP Address Range for Colocation /26 (64 addresses)

Company's Responsibilities and Included Features

- Provide an Internet routable IPv4 subnet /26 address range
- The address range provides 64 subnet addresses. Note that usable address space within that subnet will vary depending on network routing schema and Client terminating equipment.
- Maintain Internet routing tables
- Maintain all IP documentation
- Enforce IP conservation policies
- Company reserves the right to reclaim any unused address space or space that is not supplied with proper ARIN documentation.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide justification documentation for IP compliance requirements from the American Registry for Internet Numbers (ARIN).
- Stay within ARIN's usage compliance requirements
- Provide network end termination equipment within the Client environment

600441 Internet IP Address Range for Colocation /27 (32 addresses)

Company's Responsibilities and Included Features

- Provide an Internet routable IPv4 subnet /27 address range
- The address range provides 32 subnet addresses. Note that usable address space within that subnet will vary depending on network routing schema and Client terminating equipment.
- Maintain Internet routing tables
- Maintain all IP documentation
- Enforce IP conservation policies
- Company reserves the right to reclaim any unused address space or space that is not supplied with proper ARIN documentation.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide justification documentation for IP compliance requirements from the American Registry for Internet Numbers (ARIN).
- Stay within ARIN's usage compliance requirements
- Provide network end termination equipment within the Client environment

600442 Internet IP Address Range for Colocation /28 (16 addresses)

Company's Responsibilities and Included Features

- Provide an Internet routable IPv4 subnet /28 address range
- The address range provides 16 subnet addresses. Note that usable address space within that subnet will vary depending on network routing schema and Client terminating equipment.

- Maintain Internet routing tables
- Maintain all IP documentation
- Enforce IP conservation policies
- Company reserves the right to reclaim any unused address space or space that is not supplied with proper ARIN documentation.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide justification documentation for IP compliance requirements from the American Registry for Internet Numbers (ARIN).
- Stay within ARIN's usage compliance requirements
- Provide network end termination equipment within the Client environment

600443 Internet IP Address Range for Colocation /29 (8 addresses)

Company's Responsibilities and Included Features

- Provide an Internet routable IPv4 subnet /29 address range
- The address range provides 8 subnet addresses. Note that usable address space within that subnet will vary depending on network routing schema and Client terminating equipment.
- Maintain Internet routing tables
- Maintain all IP documentation
- Enforce IP conservation policies
- Company reserves the right to reclaim any unused address space or space that is not supplied with proper ARIN documentation.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide justification documentation for IP compliance requirements from the American Registry for Internet Numbers (ARIN).
- Stay within ARIN's usage compliance requirements
- Provide network end termination equipment within the Client environment

600444 Internet IP Address Range for Colocation /30 (4 addresses)

Company's Responsibilities and Included Features

- Provide an Internet routable IPv4 subnet /30 address range
- The address range provides 4 subnet addresses. Note that usable address space within that subnet will vary depending on network routing schema and Client terminating equipment.
- Maintain Internet routing tables
- Maintain all IP documentation
- Enforce IP conservation policies
- Company reserves the right to reclaim any unused address space or space that is not supplied with proper ARIN documentation.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide justification documentation for IP compliance requirements from the American Registry for Internet Numbers (ARIN).
- Stay within ARIN's usage compliance requirements
- Provide network end termination equipment within the Client environment

600639 Colocation Internet 10Gbps Port Committed

Company's Responsibilities and Included Features

Company will provide a redundant, multi-provider, managed Internet Bandwidth service to provide highly available internet access. Company will load balance traffic over multiple upstream Internet backbone providers.

- Service shall have a maximum port speed of 10Gbps.
- Service may also leverage Burstable Internet bandwidth calculated on the 95% of peak usage Item ID 600640.
- Deliver committed Internet Bandwidth allocation measured in 1 Mbps increments.
- Deliver services via fiber on single mode or multimode from redundant Internet delivery switches.
- Provide a base allocation of up to eight (8) usable via (/29 network) Internet routing IPv4 public addresses, unless the Client provides their own ASN and IPv4 portable address space.
- Provide access to upstream and downstream bandwidth usage graphs via Client portal

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Comply with Company s Acceptable Use Policy.
- Provide termination hardware for service. Requires fiber single mode or multimode termination ports.
- Notify Company if additional bandwidth is needed beyond the committed allocation.
- Commit to at least 1 Gbps of Internet bandwidth.

600640 Colocation Internet 10Gbps Port Burstable

Company's Responsibilities and Included Features

Colocation Internet Burstable Service is add-on component to Item ID 600639 Colocation Internet Committed Service..

- Client will have a maximum burst capacity of 10 Gbps.
- Bandwidth utilization in excess of the Committed Bandwidth (the minimum amount billed regardless of usage) will be billed as Burstable Bandwidth (as described below) and calculated using the 95th Percentile Method (as described below), in 1 Mbps increments
- Service shall have a maximum port speed of 10Gbps.

The 95th Percentile Method involves polling both inbound and outbound bandwidth utilization every five (5) minutes during each calendar month. All such samples are ordered from highest to lowest. The top five percent (5.0%) of readings are discarded, and Client is billed an additional charge based on the next highest reading. The amount of pre-purchased Committed Bandwidth is subtracted from the 95th Percentile to determine the Burstable Bandwidth usage to be billed. Committed Bandwidth is billed in advance; Burstable Bandwidth is billed in arrears, the month after usage occurs. In the event Client requests a hard limit higher than the Committed Bandwidth, Client agrees to be subject to the Burstable Bandwidth for bandwidth consumed beyond the Committed Bandwidth rate level on a monthly basis.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Comply with Internet acceptable use policy.
  Commit to at least 1 Gbps of Colocation Internet bandwidth Committed Item ID 600639.
- Comply with Company s Acceptable Use Policy.
- Provide termination hardware for service. Requires fiber single mode or multimode termination ports.

Category: Remote Hands

112048 Remote Hands (Block of Hours): Scheduled work Mon-Friday 8am to 5pm

Company's Responsibilities and Included Features

Provide remote hands services per Client request tracked in 15 minute increments. The hours are sold as a block, renew each month, and unused hours are not refundable or transferable at the end of each month. Remote hands services include:

- Equipment power cycling
- Secure patch cable connections
- Observation of equipment, display indicators and general environment
- Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
- Escorts of Client's unbadged vendors, employees, and auditors
- Handling of Client's media (e.g. tapes) including shipping and receiving

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Initiate a ticket or service Request for the work to be performed
- Notify Company of any special instructions for the activity

112049 Media Rotation Service

Company's Responsibilities and Included Features

Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment) Ongoing Media Rotation Service, with hand off to client specified courier. Activities are based on 15 min increments, 1 hour monthly minimum.

- Unlock and open cabinet, store media in client's colocation space
- Secure media within client s cabinet
- Rotate media
- Open support tickets to notify client in the event of errors
- Weekly/daily/monthly media swaps
- Coordinate with client s courier
- Receive container(s) from client
- Transport delivery container to client s cabinet (The client and/or 3rd party courier storage/transport containers must be appropriately marked with both receipt and return labeling.)
- Unseal delivery container
- Rotate media in back-up device with media from delivery container
- Validate tape numbers/labels for in the event of swapping multiple tapes in a library
- Seal delivery container in preparation for client pick-up
- Close ticket opened to track tape swap process
- Coordinate receipt and delivery with client s courier

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide tapes/media
- Define and documenting tape/media handling process
- Define tape/media rotation schedule
- Determining when tapes/media are replaced with new
- Test backups
- Troubleshooting and resolve tape/media backup errors/incidents
- Execute commands to eject tape/media if required (beyond pushing an external eject button)

604548 Remote Hands (Metered): Scheduled Work Monday-Friday 8AM to 5PM

Company s Responsibilities and Included Features

This SKU provides for remote hands services per Client request tracked in 15 minute increments during normal operating hours per data center. Normal operating hours are defined as 8AM-5PM Mon-Fri per data center local time. Invoicing for this service is based on the metered time the Company requires to perform the services. Remote hands services include:

- Equipment power cycling
- Secure patch cable connections
- Observation of equipment, display indicators and general environment
- Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
- Escorts of Client s unbadged vendors, employees, and auditors
- Handling of Client s media (e.g. tapes) including shipping and receiving

Client s Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Initiate a ticket or service Request for the work to be performed
- Notify Company of any special instructions for the activity

604549 Remote Hands (Metered) After Hours

Company s Responsibilities and Included Features

This SKU provides for remote hands services per Client request tracked in 15 minute increments for hours outside of normal operating hours per data center. Normal operating hours are defined as 8AM-5PM Mon-Fri per data center local time. Invoicing for this service is based on the metered time the Company requires to perform the services. Remote hands services include:

- Equipment power cycling
- Secure patch cable connections
- Observation of equipment, display indicators and general environment
- Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
- Escorts of Client s unbadged vendors, employees, and auditors
- Handling of Client s media (e.g. tapes) including shipping and receiving

Client s Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Initiate a ticket or service Request for the work to be performed
- Notify Company of any special instructions for the activity

606634 Committed Remote Hands

Company s Responsibilities and Included Features

This ItemId provides for a monthly hours of remote hands services. The quantity contracted for this ItemId is inclusive of remote hands services that are included in contracted colocation cabinets. Remote hands services include:

- Equipment power cycling
- Secure patch cable connections
- Observation of equipment, display indicators and general environment
- Physical placement of hot plug components (i.e. placement of USB and CD/DVD media into equipment)
- Escorts of Client s unbadged vendors, employees, and auditors
- Handling of Client s media (e.g. tapes) including shipping and receiving

Client s Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Initiate a ticket or service Request for the work to be performed
- Notify Company of any special instructions for the activity

Category: Setup

112028-N Standard Cabinet Setup Bundle 2.5kW Half- Cabinet

Company's Responsibilities and Included Features

Colocation Cabinet Setup Bundle includes delivery engineering and placement of the following materials:

- QTY 2 Branch Circuit Runs 208v 20A
- QTY 1 24"x 48" x 22RU Half Cabinet
- QTY 1 Ventilation Hood
- QTY 2 Dial Combo locks
- QTY 1 Up to 11RU Blanking Panels
- QTY 2 APC AP9572 C13, 4 C19

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 2500 watts (2.5 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes

112029-N Standard Cabinet Setup Bundle 5kW Cabinet

Company's Responsibilities and Included Features

Colocation Cabinet Setup Bundle includes delivery engineering and placement of the following materials:

- QTY 2 Branch Circuit Runs
- QTY 1 24"x 48" x 45RU Cabinet
- QTY 1 Ventilation Hood
- QTY 2 Dial Combo locks
- QTY 1 Up to 20 RU Blanking Panels
- QTY 2 APC AP8861 20 C13, 4 C19

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 5000 watts (5 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes

112030-N Standard Cabinet Setup Bundle 10kW Cabinet

Company's Responsibilities and Included Features

Colocation Cabinet Setup Bundle includes delivery engineering and placement of the following materials:

- QTY 4 Branch Circuit Runs 208v 30A
- QTY 1 24"x 48" x 45RU Cabinet
- QTY 1 Ventilation Hood
- QTY 2 Dial Combo locks

  QTY 1 Up to 20 RU Blanking Panels

- QTY 4 APC AP8661 20 C13, 4 C19

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 10,000 watts (10 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

112031-N Standard Cabinet Setup Bundle 15kW Cabinet

Company's Responsibilities and Included Features

Colocation Cabinet Setup Bundle includes delivery engineering and placement of the following materials:

- QTY 6 Branch Circuit Runs 208v 30A
- QTY 1 24"x 48" x 45RU Cabinet
- QTY 1 Ventilation Hood
- QTY 2 Dial Combo locks
- QTY 1 Up to 20 RU Blanking Panels
- QTY 6 APC AP8661 20 C13, 4 C19

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 15,000 watts (15 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes

500106-N Standard Cabinet Setup Bundle 4kW Cabinet

Company's Responsibilities and Included Features

Colocation Cabinet Setup Bundle includes delivery engineering and placement of the following materials

- QTY 2 Branch Circuit Runs
- QTY 1 24"x48" x 48RU Cabinet
- QTY 1 Ventilation Hood
- QTY 2 Dial Combo locks
- QTY 1 Up to 20 RU Blanking Panels
- QTY 2 APC AP8861 20 C13, 4 C19

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications

Utilize no more power than the maximum average power density as specified 4000 watts (4 kW)

- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

500107-N Standard Cabinet Setup Bundle 2kW Half-Cabinet

Company's Responsibilities and Included Features

Colocation Cabinet Setup Bundle includes delivery engineering and placement of the following materials

- QTY 2 Branch Circuit Runs 208v 20A
- QTY 1 24"x48" x 24RU Half Cabinet
- QTY 1 Ventilation Hood
- QTY 2 Dial Combo locks
- QTY 1 Up to 11RU Blanking Panels
- QTY 2 APC AP9572 C13, 4 C19

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 2000 watts (2.0 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

600325 Standard Cabinet Setup Bundle 8kW

Company's Responsibilities and Included Features

Colocation Cabinet Setup Bundle includes delivery engineering and placement of the following materials

- QTY 4 Branch Circuit Runs
- QTY 1 24"x48" x 48RU Cabinet
- QTY 1 Ventilation Hood
- QTY 2 Dial Combo locks
- QTY 1 Up to 20 RU Blanking Panels
- QTY 4 APC AP8861 20 C13, 4 C19

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 8000 watts (8 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes.

600327 Standard Cabinet Setup Bundle 2.5kW Cabinet

Company's Responsibilities and Included Features

Colocation Cabinet Setup Bundle includes delivery engineering and placement of the following materials:

- QTY 2 Branch Circuit Runs
- QTY 1 24"x 48" x 45RU Cabinet
- QTY 1 Ventilation Hood
- QTY 2 Dial Combo locks
- QTY 1 Up to 20 RU Blanking Panels
- QTY 2 APC AP8861 20 C13, 4 C19

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide all in rack infrastructure IT infrastructure
- Rack and cable the equipment
- Specify the correct circuit and plug type as required by the manufacture's specifications
- Utilize no more power than the maximum average power density as specified 2500 watts (2.5 kW)
- Client may elect to provide their own power strips within the cabinet. Client provided power strips must be UL listed and meet all applicable local and national electric codes

Family: Deal Incentives

Category: Promotional Credits

602415 Monthly Promotional Incentive - Colo

This is a placeholder for a Company service to deliver PostgreSQL administration that still needs to be developed and rolled out to Client by Company.

Contracting this ItemID does not imply any Company commitment to The delivery of this service in any specific time span.

A subsequent Change Order for this service will be issued to update the scope of services for this service.

607099 Limited Offer Discount Nutanix Xi Leap DRaaS Customers

- This offer and its features are limited to the term of this contract and may not be available after the term expires.
- This offer is exclusively applicable to current and former customers and actively engaged prospects of Nutanix s XI Disaster Recovery as a Service (DRaaS) offering.
- This offer allows the Client to run active disaster recovery supporting production and non-production workloads in the ReliaCloud DRaaS environment within the active (powered-on) capacity of the environment.
- This discount does not represent (if applicable) any other Company provided discounts for contract terms or prepayments.

Family: ERP Management

Category: Managed ERP Applications

600307 Financial Reporting

Company will provide enriched invoice data by associating Client-specific Configuration Items ("CI") or Azure resource data with standard invoice information.

Company's Responsibilities and Included Features

Invoice Data Enrichment

- Provide enriched data in mutually-agreed-upon format to support cost distribution and analysis by Client

Service Parameters

- Data will be available within five (5) working days of delivery of in-scope invoices
- This service ensures that relevant details are accurately reported based on requirements established with Client

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Service Management

- Provide Client Contact that can act as liaison between Company and Client
  - Provide requirements for invoice data enrichment
  - Coordination of validation testing
  - Accept invoice data
  - Utilize ticket system for all requests
  - Maintain Client codes and other data to be used for enrichment
- Provide accurate and up-to-date information during Client meetings, through ticket system and through documentation as may be reasonably requested by Company. Provision of incorrect information can impact data quality and timeliness of delivery
- Ensure availability of Client Contact for any discussion required for problem troubleshooting and resolution of issues

Requirements

- Collaborate with OneNeck Finance team to define, revise and enhance data requirements

Data Integrity

- Establish, review, and maintain CI and Azure data information including tagging and resource changes

Validation

- Review and accept enriched invoice data

Access and Authorization

- Provide Company access to resources and data needed to enrich invoice data
- Identify named Client users authorized to make requests or changes

Azure Subscriptions

- Client must obtain the Azure subscription(s) to be supported by Company through Company s Microsoft Cloud Service Provider program
- Service assumes existing Azure tenant and subscriptions in a stable state at onboarding. Company can provide remediation as a time and material project
- Any additional Azure resources consumed to enable troubleshooting and support such as Azure Monitor Logs and other troubleshooting resources

603840 Microsoft Dynamics Third Party Application Support

Company's Responsibilities and Included Features
Service for this Third Party Application Support will only apply to Microsoft Dynamics AX and Microsoft Dynamics 365 applications.

Application User Administration

Management of user identities within the application:

- User ID adds, changes, deletes
- Security group/role maintenance as applicable to the application as defined by the Client

Incident Triage and Resolution

Company will triage and manage the troubleshooting process for technical system errors.
Company will research problems and issues utilizing:

- Company knowledge of known errors and their solution
- General operating system level troubleshooting
- Escalation to software provider

Resolution of system incidents:

- Application of Company known solutions
- Application of software vendor provided solutions

Engagement of software providers Help Desk support
Document user issues and system errors

Patching and Upgrades

Standard Patch Maintenance - Company shall provide patch application where patches for the application are within the following criteria:

- One-off patches - Patch to address a specific failure to standard functionality (i.e. Break-Fix)
- Any single or group of patches (Service Pack) required to solve a single issue or required by software vendor
- The patching activity is not associated with an application version upgrade

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

Development Support

Provide application development resources to develop new or modify existing configurations, extensions, modifications,

localizations and integrations

- Develop technical specification based upon functional requirements
- Develop or modify application objects
- Develop or modify reports
- Conduct unit and integration testing
- Document customizations

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Performance Tuning

- Provide application performance tuning

606982 Dynamics 365 Financial and Operations - On Premise - Batch Administration and Monitoring

Company's Responsibilities and Included Features

General

Company will provide batch management, application monitoring and of one (1) Dynamics 365 Financial and Operations cloud environment as described herein.

Batch Management

- Create batch jobs based on criteria provided by Client
- Update batch jobs based on criteria provided by Client
- Triage and assist with the troubleshoot and optimization of batches

Application Monitoring

- Batch jobs
- Dynamics 365 license counts
- Number sequences
- User session status

Dynamics 365 Technical Expert to Expert Support

- 24x7 for high priority batch Job issues (P1-P2 Alerts)
- 8x5 for Company standard monitoring alerts(P3-P5)

Dynamics 365 Functional Support

- Implement, manage, and monitor weekly aging

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Functional design of batch jobs
- AX modules and 3rd party application support
- Application software licensing
- End user support and management

Application functional support
- Application development
- Database management
- Performance tuning

Category: Microsoft Enterprise Applications

600002 Microsoft Dynamics AX additional module application support

Company's Responsibilities and Included Features

Incident Triage and Resolution

Company will triage and manage the troubleshooting process for technical system errors.
Company will research problems and issues utilizing:

- Company knowledge of known errors and their solution
- General operating system level troubleshooting
- Escalation to software provider

Resolution of system incidents:

- Application of Company known solutions
- Application of software vendor provided solutions

Engagement of software providers Help Desk support
Document user issues and system errors

Microsoft Dynamics Additional Module Patching and Upgrades

Standard Patch Maintenance - Company shall provide patch application patches for Microsoft Dynamics AX additional modules as identified in the Service Description in Pricing Parameters within the following criteria:

- One-off patches - Patch to address a specific failure to standard functionality (i.e. Break-Fix)
- Any single or group of Microsoft Dynamics AX additional module patches (Service Pack) required to solve a single or multiple failures to standard functionality
- Hot-fix roll-ups
- The patching activity is not associated with an Microsoft Dynamics AX version or Microsoft Dynamics AX additional module version upgrade
- The patching activity is not associated with an Microsoft SQL Database version upgrade

Advanced Patch Management - Company shall provide patch application for customized code where patches for Microsoft Dynamics AX additional modules are
within the following criteria:

- One-off patches - Patch to address a specific failure to customized functionality (i.e. Break-Fix)
- Any single or group of customized Dynamics AX additional module code patches required to solve a single or multiple failures to customized functionality
- The patching activity is not associated with an Microsoft Dynamics AX version or Microsoft Dynamics AX additional module version upgrade
- The patching activity is not associated with an Microsoft SQL Database version upgrade

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents

- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

600003 Microsoft Dynamics AX System Administration Support

Company's Responsibilities and Included Features

Provide application support for the areas listed within the Company responsibilities, limited to the number of contracted support hours per month.

Application Administration

Manage the following areas within the Dynamics AX Applications suite:

- User provisioning and security within AX (excluding user active directory provisioning)
- Services Monitoring
- Cloning environments
- Clone application and refresh database from production to non-production environment.
- Quantity of clones provided is referenced in the Service Parameters

Printers and queues Batch management Password management for Administrators

Custom object change management:

- Migration of customizations through Development, Test, QA environments (as applicable) through to production
- Change control

Modules Supported:

- All Dynamics AX Modules built in to the Dynamics AX platform (binaries) will be supported.The Default CRM function built in AX 20xx would be an included supported module. The Dynamics CRMxx product as a Stand Alone application would be considered out of scope of this service.
- Enterprise Portal:
- If included, as referred to as "Number of Enterprise Portal servers" in Pricing Parameters

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Engagement of software providers Help Desk support (requires Client to have a support contract with the software

provider)

- Where necessary Company will engage and log service requests with the software vendor to rectify software issues
- Provide client with updates

Document user issues and system errors

Patching and Upgrades

Standard Patch Maintenance - Company shall provide patch application where patches for Microsoft Dynamics AX are within the following criteria:

- One-off patches - Patch to address a specific failure to standard functionality (i.e. Break-Fix)
- Any single or group of Microsoft Dynamics AX patches (Service Pack) required to solve a single or multiple failures to standard functionality
- Hot-fix roll-ups or kernel only updates
- The patching activity is not associated with an Microsoft Dynamics AX version upgrade
- The patching activity is not associated with an Microsoft SQL Database version upgrade

Advanced Patch Management - Company shall provide patch application for customized code where patches for Microsoft Dynamics AX are
within the following criteria:

- One-off patches - Patch to address a specific failure to customized functionality (i.e. Break-Fix)
- Any single or group of customized Dynamics AX code patches required to solve a single or multiple failures to customized functionality
- The patching activity is not associated with an Microsoft Dynamics AX version upgrade
- The patching activity is not associated with an Microsoft SQL Database version upgrade

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Advanced AX modules and 3rd Party Application Support

The following modules or functionality are not included in the scope of this Service Item but can be supported under additional Service Items:

- Business intelligence and reporting (including Microsoft FRx, Microsoft SQL Reporting Services and Analysis Services)
- Client Relationship Management
- Application Integration Framework
- Microsoft SQL Integration Services
- Third Party applications or modules.

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

End user Support and Management

- Support of non-super users
- Application functional support
- Application Development

600123 Microsoft Dynamics AX production system administration

Company's Responsibilities and Included Features

Application Administration

Manage the following areas within the Dynamics AX Applications suite:

- User provisioning and security within AX (excluding user active directory provisioning)
- Services Monitoring
- Cloning environments
- Clone application and refresh database from production to non-production environment.
- Quantity of clones provided is referenced in the Service Parameters
- Printers and queues
- Batch management
- Password management for Administrators

Custom object change management:

- Migration of customizations through Development, Test, QA environments (as applicable) through to production
- Change control

Modules Supported:

- All Dynamics AX Modules built in to the Dynamics AX platform (binaries) will be supported.The CRM function built in Dynamics AX would be an included supported module. The Dynamics CRM product as a standalone application would be considered out of scope of this service
- Enterprise Portal, if included, as referred to as "Number of Enterprise Portal servers" in Pricing Parameters

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Engagement of software providers Help Desk support (requires Client to have a support contract with the software provider)
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues
- Provide client with updates
- Document user issues and system errors

Patching and Upgrades

Standard Patch Maintenance - Company shall provide patch application where patches for Microsoft Dynamics AX are within the following criteria:

- One-off patches - Patch to address a specific failure to standard functionality (i.e. Break-Fix)
- Any single or group of Microsoft Dynamics AX patches (Service Pack) required to solve a single or multiple failures to

standard functionality
- Hot-fix roll-ups or kernel only updates
- The patching activity is not associated with an Microsoft Dynamics AX version upgrade
- The patching activity is not associated with an Microsoft SQL Database version upgrade

Advanced Patch Management - Company shall provide patch application for customized code where patches for Microsoft Dynamics AX are within the following criteria:

- One-off patches - Patch to address a specific failure to customized functionality (i.e. Break-Fix)
- Any single or group of customized Dynamics AX code patches required to solve a single or multiple failures to customized functionality
- The patching activity is not associated with an Microsoft Dynamics AX version upgrade
- The patching activity is not associated with an Microsoft SQL Database version upgrade

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Advanced AX modules and 3rd Party Application Support

The following modules or functionality are not included in the scope of this Service Item but can be supported under additional Service Items:

- Business intelligence and reporting (including Microsoft FRx, Microsoft SQL Reporting Services and Analysis Services)
- Client Relationship Management
- Application Integration Framework
- Microsoft SQL Integration Services
- Third Party applications or modules
- Microsoft Dynamics CRM

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

End user Support and Management

- Support of non-super users
- Application functional support
- Application Development

600128 Microsoft Dynamics AX disaster recovery application administration

Company's Responsibilities and Included Features

General

- Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center.
- This service is specific to the administration of a Microsoft Dynamics AX environment in a Recovery Site acting as a failover environment.
- Replication of the application binaries and file systems from the primary servers to the target DR servers is to be provided through the use of server to server replication software and requires an OS replication Service Item which will perform the replication.
- Company shall develop and maintain Disaster Recovery Failover Procedures.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Application Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client
- The number of failover tests per year is referenced in Pricing Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the data was when testing began.

Application Failover Services

- On declaration of a disaster, Company will perform the steps necessary to restart and validate the application on the target DR server and make it the primary application environment, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the primary environment, administration of the Dynamics AX application will be as per the administrative, support, backup and monitoring services as defined for the primary environment.
- Server Failback Services will be provided on a project, time and material basis

Application Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The application administrator will assist the operating systems administrator reestablish application file system replication back to the target DR server.
- Application Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Third Party Application Dependency Management

- Management of third party application interface to the application
- Administration of third party applications associated with this DR environment.

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

600161 Microsoft Dynamics AX non-production system administration

Company's Responsibilities and Included Features

Application Administration

Manage the following areas within the Dynamics AX Applications suite:

- User provisioning and security within AX (excluding user active directory provisioning)
- Services Monitoring
- Cloning environments
- Clone application and refresh database from production to non-production environment.
- Quantity of clones provided is referenced in the Service Parameters
- Printers and queues
- Batch management
- Password management for Administrators

Custom object change management:

- Migration of customizations through Development, Test, QA environments (as applicable) through to production
- Change control

Modules Supported:

- All Dynamics AX Modules built in to the Dynamics AX platform (binaries) will be supported.The CRM function built in Dynamics AX would be an included supported module. The Dynamics CRM product as a standalone application would be considered out of scope of this service
- Enterprise Portal, if included, as referred to as "Number of Enterprise Portal servers" in Pricing Parameters

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Engagement of software providers Help Desk support (requires Client to have a support contract with the software provider)
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues
- Provide client with updates
- Document user issues and system errors

Patching and Upgrades

Standard Patch Maintenance - Company shall provide patch application where patches for Microsoft Dynamics AX are within the following criteria:

- One-off patches - Patch to address a specific failure to standard functionality (i.e. Break-Fix)
- Any single or group of Microsoft Dynamics AX patches (Service Pack) required to solve a single or multiple failures to standard functionality
- Hot-fix roll-ups or kernel only updates
- The patching activity is not associated with an Microsoft Dynamics AX version upgrade
- The patching activity is not associated with an Microsoft SQL Database version upgrade

Advanced Patch Management - Company shall provide patch application for customized code where patches for Microsoft Dynamics AX are within the following criteria:

- One-off patches - Patch to address a specific failure to customized functionality (i.e. Break-Fix)
- Any single or group of customized Dynamics AX code patches required to solve a single or multiple failures to customized functionality
- The patching activity is not associated with an Microsoft Dynamics AX version upgrade
- The patching activity is not associated with an Microsoft SQL Database version upgrade

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Advanced AX modules and 3rd Party Application Support

The following modules or functionality are not included in the scope of this Service Item but can be supported under additional Service Items:

- Business intelligence and reporting (including Microsoft FRx, Microsoft SQL Reporting Services and Analysis Services)
- Client Relationship Management
- Application Integration Framework
- Microsoft SQL Integration Services
- Third Party applications or modules
- Microsoft Dynamics CRM

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

End user Support and Management

- Support of non-super users
- Application functional support
- Application Development

600250 Dynamics AX Architecture Advisory Services

Company's Responsibilities and Included Features

Company will provide guidance on suitability, architectural alternatives and ability for the Client s Microsoft Dynamics AX environment to support the Client s business requirements, goals, and plans during their Dynamics AX implementation project and in production.

During the Client s Dynamics AX implementation project, Company shall provide architecture advisory services through scheduled periodic meetings with the Client and Client s partner. Company will provide feedback, advice, and recommendations during the periodic meetings, and will also work outside of the meetings to research, investigate, prepare additional recommendations.

Topics for analysis and/or recommendations within which the Dynamics AX Architecture Advisory Services can be delivered:

- Independent Software Vendor (ISV) solutions integrated into Dynamics AX
- Data integrations (SaaS, EDI, etc.) type and volume
- Volume of transactions by type (Examples - sales orders, purchase orders, production orders)

Number and type of users concurrent and named
- Location of users
- Expensive workloads (MRP, Cost rollups, invoice batching)
- Data warehousing/BI
- DR/BC
- Enterprise Portal/Role Center usage
- Retail configuration
- Handheld device usage
- Client access method
- High availability architecture
- Code promotion strategy
- Data refresh strategy
- Backup strategy (Types of backup, retention, location)
- Average line items per transactions
- Organic business growth versus acquisitions and the impact on the architecture
- Data migration strategy

This service is delivered as a block of hours available for consumption within the monthly billing period. Unconsumed hours do not roll-over to subsequent months.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Client must provide complete documentation of their existing or planned Microsoft Dynamics AX architecture, including a logical and physical layout of the solution architecture, a list of server roles and specifications/sizing, storage and networking specifications, and connectivity strategy. If Client does not have the requirement documentation, Company can create it through a separate engagement.
- Engage with Company in the periodic meetings.
- Provide necessary data to enable meaningful analysis and subsequent recommendations.

601250 Dynamics 365 Financial and Operations Application Administration

Services Scope and Responsibilities

The following Responsibility Matrix defines the scope and assigns responsibility for each task required for the management of Client's Dynamics 365 environments. SI/ISV refers to the applicable system integrator or integrated software vendor

Responsibilities Matrix Legend		
R	**Responsible**	Party that performs a tasks
A	**Accountable**	Party that is ultimately accountable for the task and has approval and veto authority for the task
C	**Consulted**	Party from whom reasonable feedback and contribution to the task is required
I	**Informed**	Party that requires knowledge of the outcome of the task

Responsibilities Matrix

		Party Assignments			

Task; Item	Notes; Actions Required	Microsoft	Company	SI/ISV	Client
User Management					
User account modifications	Changes to user setup options include modifications to visual interface, preferences, user account, and workflow settings.		RA		C
User account importation/creation			RA		C
Worker record creation and association to user			RA		C
Troubleshoot user options and personalization	Includes SQL statement tracing, deadlock tracing, and assistance/troubleshooting with form personalization. Targeted deletion of user s usage data (corrupted personalization or filters/queries), clearing of user s usage data and cache files, and similar tasks.		RA		C
Set up user options and personalization	Includes tracing values and toolbar setup.		RA		C
Licensing			I		RA
Dynamics 365 Security					
Assign security roles/groups			R		A
Define security roles/groups	Company can assist with this task on a time and material project basis.		I		RA
Develop/deploy security roles based on criteria provided by Client	This task will be provided on a time and material project basis.		R		A
Batch Management					
Functionally design batch jobs			I	C	RA
Create batch jobs based on criteria provided by Client			R		A
Update batch jobs based on criteria provided by Client			R		A
Triage and assist with the troubleshoot and optimization of batches			R		A
Organization Administration					
Number sequence configurations			I	C	RA
Manage network printers with Document Routing Agent (DRA)	Customer will need to assist in install/setup DRA to each print server, or provide access to Company. DRA requires periodic maintenance, i.e. 90 day user token and on service updates.		R		A
Change Management					

Manage code promotion process			R		A
Submit code package to production environment (up to 1 promotion per week)		R	A		C
Submit code package to sandbox environment (up to 1 promotion per week)			RA		C
Develop code objects via Azure DevOps					RA
Install platform updates to production environment		RA	I		I
Install platform updates to development environment					RA
Install platform updates to sandbox environment			RA		C
Test platform updates					RA
System Administration					
Data refresh of sandbox environments on an ad-hoc or automated schedule basis as mutually agreed			RA		C
Data refresh of non-production environments on an ad-hoc or automated schedule basis as mutually agreed			C		RA
Code regression to non-production environments on an ad-hoc basis					RA
Restart of sandbox environment AOS service			RA		C
Restart of development environment AOS service			C		RA
Track and manage Microsoft Technical Support Request (MTSR)		C	R		A
Periodically review system health	Limited to configuration and performance data collected via readily available tools (i.e., LCS and PowerShell) compared against Microsoft or Company documented best practices.		RA		I
Manage Lifecycle Services (LCS)	Includes request and scheduling of code promotions and environment refreshes, and review of diagnostics, telemetry and monitoring.		RA		I

Database Maintenance					
Manage SQL sessions	Company can only kill SPIDs from LCS	RA	C		I
Review table sizes/opportunities for purging/archiving			R		A
Maintain log/database files		RA			
Setup SQL agent jobs to support application		RA			
Shoulder Application Support (contracted separately)					
General administration			RA		C
Application installation			RA		C
Administer upgrades and patching			R		A
User provisioning and manage security			RA		C
Troubleshoot application platform			RA		C
Integration support			R		A
Application Monitoring					
Services: AOS		RA			
Services: shoulder applications native to Dynamics 365		RA	I		I
Services: shoulder applications external to Dynamics 365			RA		I
Batch jobs			R		A
Dynamics 365 user counts		C	R		A
Number sequences			R		A
User session status			RA		I
Financial Reporter (formerly Management Reporter)		RA			
Additional custom monitoring	This task will be provided on a time am material basis		RA		C
Performance Tuning					
Index analysis		RA			C
SQL server instance configuration		RA			
Manage AOS configuration			RA		C

High-level code review	Restricted to troubleshooting performance issues. Review of issues found, or implementation of suggestions made, by Company are the responsibility of Client.		C		RA
Dynamics 365 architecture and infrastructure review		RA	C		A
Dynamics 365 Technical Expert to Expert Support					
24x7 for high priority issues (P1-P2)		C	RA		C
8x5 for standard issues and requests (P3-P5)		C	RA		C
Incident triage, troubleshoot and solution recommendations		C	RA		C
Application crash dump collection and diagnostics		RA	I		C
Dynamics 365 functional support					
Finance functional support				R	A
Human Capital Management (HCM) functional support				R	A
Project functional support				R	A
Trade and logistics functional support				R	A
Retail functional support				R	A
Incident triage, troubleshoot and solution recommendations			RA		C
Escalate issues outside of scope to appropriate resource (Client/VAR/Microsoft)			RA		C
Adjust/extend number sequences based on Client input			R		AC
Implement, manage, and monitor custom critical business process			R		A
Configure and troubleshoot workflow functionality			R		A
Configure and troubleshoot Dynamics 365 alert system functionality			R		A
Installation and Configuration of Dynamics 365 Components					

Database		RA	I		I
AOS		RA	I		I
SQL Server Reporting Services (SSRS)		RA	I		I
Power platform		RA	I		I
Functional Implementation					
New implementation		C	C	R	A
Implement new functionality			C	R	A
Functional design of customizations			I	R	A
Custom Development					
Technical design of customizations				R	A
Code development				R	A
Deep dive code review				R	C
Application Integration Framework (AIF) and Common Data Model (CDM) integrations			C	R	A

Service Limits

The scope of services is limited to:

Administration of two environments:

- One production environment
- One sandbox environment

A maximum of 100 concurrent users. Additional users can be contracted under ItemID 601251 - Dynamics 365 Financial and Operations Application Management - Additional Users

Additional Client Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Advanced AX Modules and 3rd Party Application Support

The following modules and functionalities are not included in the scope of this Service Item, but can be supported under other Service Items:

- Business intelligence and reporting (including Microsoft Management Reporter, Microsoft SQL Reporting Services and analysis services)
- Application integration framework
- Microsoft SQL integration services
- Third party applications or modules
- Microsoft Dynamics CRM

Application Software Licensing

- Procure application software and licensing for current version on current operating system, including any user/administrator or processor access licensing
- Provide software media for installation, maintenance and configuration of the application
- Procure current software support and maintenance where applicable

End User Support and Management

- Support of non-super users
- Application functional support
- Application development

601251 Dynamics 365 Financial and Operations Application Management - Additional Users

Services Scope and Responsibilities

Provide additional users to the scope of ItemID 601250 - Dynamics 365 Financial and Operations Application Administration to increase the maximum concurrent user limit

Additional Client Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

None

601481

Services Scope and Responsibilities

Provide additional users to the scope of ItemID 601480 - Dynamics 365 Financial and Operations - On Premise - Application Administration to increase the maximum concurrent user limit

Additional Client Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

None

Category: Oracle Enterprise Applications

600010 Oracle ASCP application administration

Company's Responsibilities and Included Features

Application Administration

Manage the following areas within the Oracle Advanced Supply Chain Planning (ASCP) Application:

- Security management
    - Group Management
    - User mangement
    - Menu security management
    - Application log monitoring
- Batch monitoring
- Cloning environments* - limited 1 per month

Custom object change management:

- Migration of customizations through development, test, QA environments (as applicable) through to production
- RICE objects, including package build and deploy
- Change control

24x7x365 Help desk support

* Requires a 5 business day notification for planning.

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Engagement of software providers Help Desk support (requires Client to have a support contract with the software provider)
    - Where necessary Company will engage and log service requests with the software vendor to rectify software issues
    - Provide client with updates
- Document user issues and system errors

Patching and Upgrades

Application patching includes research and application of critical updates, recommended patches, updates, and security patches

Break-Fix Patching - Break-Fix patch application will follow the incident priority response SLA

ASCP Break-Fix patching is defined as - A patch or series of patches required by Oracle to rectify an error in the application code of Oracle ASCP functionality that has already been implemented, tested and is in production in the Client's environment and include any individual patches, dependent patch sets, required to addressed cuClientpecific ASCP application issues in functionality that has already been implemented, tested and is in production in the custClientvironment, and any Oracle recommended critical CU, Mini-pack or Family-pack needed to address known issues affecting a customClientronment

Non Break-Fix Patching - Non Break-Fix patching requires a 5 business day notification for planning.

The following are types of patches which are not deemed to be Non Break-Fix:

- New functionality
- New architecture
- New modules
- Minor and major version upgrades
- Quarterly Consolidated Patch Upgrade (CPU)
- Maintenance Release
- Family Pack
- Consolidated Update (CU)
- Product Mini-Pack

Major Version Upgrades - Any major version upgrades, will be treated on a time and material basis and shall be planned and billed to Client as agreed upon by the Parties

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Data and Planning Administration

Manage the following areas within the Oracle ASCP Application:

- Data management
- Workflow management
- Batch configuration
- Configuring and running Collections
- Analytical engine configuration.

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

600130 Oracle Discoverer disaster recovery application administration

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of an Oracle Business Intelligence Discoverer environment in a Recovery Site acting as a failover environment.

Replication of the application binaries and file systems from the primary servers to the target DR servers is to be provided through the use of server to server replication software and requires an OS replication Service Item which will perform the replication.

Company shall develop and maintain Disaster Recovery Failover Procedures.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Application Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client
- The number of failover tests per year is referenced in Pricing Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the

data was when testing began.

Application Failover Services

On declaration of a disaster, Company will perform the steps necessary to restart and validate the application on the target DR server and make it the primary application environment, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.

During the period that the target DR server is acting as the primary environment, administration of the Oracle EBS application will be as per the administrative, support, backup and monitoring services as defined for the primary environment.

Application Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The application administrator will assist the operating systems administrator reestablish application file system replication back to the target DR server.
- Application Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Third Party Application Dependency Management

- Management of third party application interface to the application
- Administration of third party applications associated with this DR environment.

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

600134 Oracle OBIEE disaster recovery application administration

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of an Oracle Business Intelligence Enterprise Edition (OBIEE) environment in a Recovery Site acting as a failover environment.
Replication of the application binaries and file systems from the primary servers to the target DR servers is to be provided through the use of server to server replication software and requires an OS replication Service Item which will perform the replication.
Company shall develop and maintain Disaster Recovery Failover Procedures.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Application Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client
- The number of failover tests per year is referenced in Pricing Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the data was when testing began.

Application Failover Services

On declaration of a disaster, Company will perform the steps necessary to restart and validate the application on the target DR server and make it the primary application environment, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
During the period that the target DR server is acting as the primary environment, administration of the Oracle EBS application will be as per the administrative, support, backup and monitoring services as defined for the primary environment.

Application Failback Services

When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.

- The application administrator will assist the operating systems administrator reestablish application file system replication back to the target DR server.
- Application Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Third Party Application Dependency Management

- Management of third party application interface to the application
- Administration of third party applications associated with this DR environment.

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents

- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

600135 Oracle EBS disaster recovery application administration

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of an Oracle EBS environment in a Recovery Site acting as a failover environment.

Replication of the application binaries and file systems from the primary servers to the target DR servers is to be provided through the use of server to server replication software or SAN replication and requires a replication Service Item which will perform the replication.

Company shall develop and maintain Disaster Recovery Failover Procedures.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Application Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client
- The number of failover tests per year is referenced in Pricing Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the data was when testing began.

Application Failover Services

On declaration of a disaster, Company will perform the steps necessary to restart and validate the application on the target DR server and make it the primary application environment, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.

During the period that the target DR server is acting as the primary environment, administration of the Oracle EBS application will be as per the administrative, support, backup and monitoring services as defined for the primary environment.

Application Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The application administrator will assist the operating systems administrator reestablish application file system replication back to the target DR server.
- Application Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Third Party Application Dependency Management

- Management of third party application interface to the application
- Administration of third party applications associated with this DR environment.

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

600136 Oracle ASCP disaster recovery application administration

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of an Oracle Advances Supply Chain Planning (ASCP) environment in a Recovery Site, acting as a failover environment.

Replication of the application binaries and file systems from the primary servers to the target DR servers is to be provided through the use of server to server replication software and requires an OS replication Service Item which will perform the replication.
Company shall develop and maintain Disaster Recovery Failover Procedures.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Application Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client
- The number of failover tests per year is referenced in Appendix E - Service Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the data was when testing began.

Application Failover Services

On declaration of a disaster, Company will perform the steps necessary to restart and validate the application on the target DR server and make it the primary application environment, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
During the period that the target DR server is acting as the primary environment, administration of the Oracle Demantra application will be as per the administrative, support, backup and monitoring services as defined for the primary environment.

Application Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The application administrator will assist the operating systems administrator reestablish application file system replication back to the target DR server.
- Application Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The

number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Third Party Application Dependency Management

- Management of third party application interface to the application
- Administration of third party applications associated with this DR environment.

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

600137 Oracle Demantra disaster recovery application administration

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of an Oracle Demantra environment in a Recovery Site acting as a failover environment.
Replication of the application binaries and file systems from the primary servers to the target DR servers is to be provided through the use of server to server replication software and requires an OS replication Service Item which will perform the replication.
Company shall develop and maintain Disaster Recovery Failover Procedures.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the

network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Application Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client
- The number of failover tests per year is referenced in Pricing Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the data was when testing began.

Application Failover Services

On declaration of a disaster, Company will perform the steps necessary to restart and validate the application on the target DR server and make it the primary application environment, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
During the period that the target DR server is acting as the primary environment, administration of the Oracle Demantra application will be as per the administrative, support, backup and monitoring services as defined for the primary environment.

Application Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The application administrator will assist the operating systems administrator reestablish application file system replication back to the target DR server.
- Application Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Third Party Application Dependency Management

- Management of third party application interface to the application
- Administration of third party applications associated with this DR environment.

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

600138 Oracle Agile PLM disaster recovery application administration

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of an Oracle Agile environment in a Recovery Site acting as a failover environment.
Replication of the application binaries and file systems from the primary servers to the target DR servers is to be provided through the use of server to server replication software and requires an OS replication Service Item which will perform the replication.
Company shall develop and maintain Disaster Recovery Failover Procedures.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Application Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client

The number of failover tests per year is referenced in Pricing Parameters

- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the data was when testing began.

Application Failover Services

On declaration of a disaster, Company will perform the steps necessary to restart and validate the application on the target DR server and make it the primary application environment, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.

During the period that the target DR server is acting as the primary environment, administration of the Oracle Agile application will be as per the administrative, support, backup and monitoring services as defined for the primary environment.

Application Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The application administrator will assist the operating systems administrator reestablish application file system replication back to the target DR server.
- Application Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application

- Procurement of current software support and maintenance where applicable

Third Party Application Dependency Management

- Management of third party application interface to the application
- Administration of third party applications associated with this DR environment.

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

600169 Oracle Demantra application administration

Company's Responsibilities and Included Features

Application Administration

Manage the following areas within the Oracle Demantra Applications suite:

- Security management
- Group Management
- User mangement
- Menu security management
- Application log monitoring
- Batch monitoring

Cloning environments - limited to the number of clones as referenced in Pricing Parameters
Custom object change management:

- Migration of customizations through development, test, QA environments (as applicable) through to production
- RICE objects, including package build and deploy
- Change control

24x7x365 Help desk support
* Requires a 5 business day notification for planning.

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Engagement of software providers Help Desk support (requires Client to have a support contract with the software provider)
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues
- Provide client with updates

Document user issues and system errors

Patching and Upgrades

Application patching includes research and application of critical updates, recommended patches, updates, and security patches
Break-Fix Patching - Break-Fix patch application will follow the incident priority response SLA
Demantra Break-Fix patching is defined as - A patch or series of patches required by Oracle to rectify an error in the application code of Oracle Demantra functionality that has already been implemented, tested and is in production in the Client's environment and include any individual patches, dependent patch sets, required to addressed cuClientpecific Demantra

application issues in functionality that has already been implemented, tested and is in production in the custClientvironment, and any Oracle recommended critical CU, Mini-pack or Family-pack needed to address known issues affecting a customClientronment
Non Break-Fix Patching - Non Break-Fix patching requires a 5 business day notification for planning.
The following are types of patches which are not deemed to be Non Break-Fix:

- New functionality
- New architecture
- New modules
- Minor and major version upgrades
- Quarterly Consolidated Patch Upgrade (CPU)
- Maintenance Release
- Family Pack
- Consolidated Update (CU)
- Product Mini-Pack

Major Version Upgrades - Any major version upgrades, will be treated on a time and material basis and shall be planned and billed to Client as agreed upon by the Parties

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Data and Planning Administration

Manage the following areas within the Oracle Demantra Applications suite:

- Data management
- Workflow management
- Worksheet management
- Analytical Engine configuration, tuning and running

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management

End user client software support

600170 Oracle Agile PLM application administration

Company's Responsibilities and Included Features

Application Administration

Manage the following areas within the Oracle Agile PLM Applications suite:

- Security management
- Group management
- User management

Cache management Application log monitoring Cloning environments - limited to the number of clones as referenced in Pricing Parameters

Custom object change management:

- Migration of customizations through development, test, QA environments (as applicable) through to production
- RICE objects, including package build and deploy
- Change control

24x7x365 Help desk support

* Requires a 5 business day notification for planning.

Incident Diagnosis and Troubleshooting

- Diagnosis of system incidents
- Troubleshooting of system incidents
- Engagement of Oracle support
- Where necessary Company will engage and log service requests with Oracle to rectify software issues
- Provide client with updates

Document user issues and system errors

Patching and Upgrades

Application patching includes research and application of critical updates, recommended patches, updates, and security patches

Break-Fix Patching - Break-Fix patch application will follow the incident priority response SLA

Agile Break-Fix patching is defined as - A patch or series of patches required by Oracle to rectify an error in the application code of Oracle Agile PLM functionality that has already been implemented, tested and is in production in the Client's environment and include any individual patches, dependent patch sets, required to addressed Client specific Agile application issues in functionality that has already been implemented, tested and is in production in the custClientvironment, and any Oracle recommended critical CU, Mini-pack or Family-pack needed to address known issues affecting a customClientronment

Non Break-Fix Patching - Non Break-Fix patching requires a 5 business day notification for planning.

The following are types of patches which are not deemed to be Non Break-Fix:

- New functionality
- New architecture
- New modules
- Minor and major version upgrades
- Quarterly Consolidated Patch Upgrade (CPU)
- Maintenance Release
- Family Pack
- Consolidated Update (CU)
- Product Mini-Pack

Major Version Upgrades - Any major version upgrades, will be treated on a time and material basis and shall be planned and billed to Client as agreed upon by the Parties

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Data and Product Administration

Manage the following areas within the Oracle Agile PLM Applications suite:

- Core Data management
- Document Reference Library (DRL) data
- Global Specification Management (GSM) data
- New Product Development (NPD) data
- Product Quality Scorecard (PQS) data
- Supply Chain Relationship Management (SCRM) data

Workflow management Cache management

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

600171 Oracle Essbase application administration

Company's Responsibilities and Included Features

Essbase Application Administration

Essbase application administaration includes the following areas:

- Data imports into Essbase
- Data dumps and reload
- Cube reorganizations
- Application software break-fix with escalation through to software vendor where necessary
- Database interaction and connection configuration
- Optimization of caches and buffers
- Managing and scheduling of data loading tasks

- Scheduling of cube exports as needed

User Access

- Security management
- New User ID s and passwords (upon written request by the Client)
- Essbase Security Supervisor
- Maintain User ID s and the Essbase Application Manager
- Hyperion Reports Administration utilities
- Managing Client data
- User/Group Application Access and resetting of User ID passwords

Batch Jobs Maintenance and Creation

- Maintenance for existing non-interactive applications (Batch Jobs)
- Monitor the delivery of Batch Jobs: execution time and amount of server resources
- Update minor changes
- Create and place Batch Jobs into production (based on Client requirements)
- Create and test Batch Job in Essbase as appropriate

Upgrade and Patch Management

- Periodic review of critical patches
- Up to quarterly routine review same version patch analysis and application
- Application of same version updates and patches during approved maintenance windows
- Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Issue Resolution / Solution Research / Solution Implementation

- Logging all user issues and assign priority levels
- Research problems and issues utilizing general trouble shooting and Hyperion Global Support
- Solution of an identified problem and appropriate action with notification to Client
- System Administration assistance to Client in developing work-arounds to issues

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing

- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Essbase Application Content Management, Configuration and Development

- Existing or new customized report development or maintenance
- New cube development
- Database content management
- Data extraction from source
- Third-party application integration
- Domain user administration
- Backups of data
- Usability and configuration documentation

End User Support and Management

- Support of non-expert users
- Application functional support

600183 Oracle Business Intelligence Discoverer application administration

Company's Responsibilities and Included Features

General

Oracle Business Intelligence Discoverer application administration is provided where Discoverer is used soley for reporting of Oracle EBS data

- Manage the following areas within the application:
- User security group/role maintenance within the application as defined by the Client
- Application monitoring
- Starting, stopping and restarting services.

24x7x365 Help desk support

Incident Triage and Resolution

Company will triage and manage the troubleshooting process for technical system errors.
Company will research problems and issues utilizing:

- Company knowledge of known errors and their solution
- General operating system level troubleshooting
- Escalation to software provider

Resolution of system incidents:

- Application of Company known solutions
- Application of software vendor provided solutions

Engagement of software providers Help Desk support
Document user issues and system errors

Patching and Upgrades

Standard Patch Maintenance - Company shall provide patch application where patches for the application are within the following criteria:

- One-off patches - Patch to address a specific failure to standard functionality (i.e. Break-Fix)
- Any single or group of patches (Service Pack) required to solve a single issue or required by software vendor
- The patching activity is not associated with an application version upgrade

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Development Support

Provide application development resources to develop new or modify existing configurations, extensions, modifications, localizations and integrations

- Develop technical specification based upon functional requirements
- Develop or modify application objects
- Develop or modify reports
- Conduct unit and integration testing
- Document customizations

600184 Oracle EBS application administration

Company's Responsibilities and Included Features

Application Administration

Manage the following areas within the Oracle Applications suite:

- Instance management
- Cloning environments - limited to one clone per instance per month
- Oracle Workflow
- Notification Mailer
- Concurrent Managers
- Printers and queues
- Password management for Administrators
- Load Balancers

Custom object change management:

- Migration of customizations through development, test, QA environments (as applicable) through to production
- RICE objects, including package build and deploy
- Change control

24x7x365 Help desk support
* Requires a 5 business day notification for planning.

Incident Diagnosis and Troubleshooting

- Diagnosis of system incidents
- Troubleshooting of system incidents
- Engagement of Oracle support
- Where necessary Company will engage and log service requests with Oracle to rectify software issues
- Provide client with updates
- Document user issues and system errors

Patching and Upgrades*

Break-Fix Patching - Break-fix patch application will follow the incident priority response SLA

- A Break-Fix patch is defined as a patch or series of patches required by Oracle to rectify an error in the application code to Oracle EBS that has already been implemented, tested and is in production in the Client's environment

Non Break-Fix Patching - The following are types of patches which are not deemed to be Break-Fix:

- New functionality
- New architecture
- New modules
- Minor and major version upgrades
- Quarterly Consolidated Patch Upgrade (CPU)
- Maintenance Release
- Family Pack
- Consolidated Update
- Product Mini-Pack

Requires a 5 business day notification for planning
*Patch application is limited to the number of hours per month as shown in Pricing Parameters calculated on a 3 month rolling average
Patch application includes research and installation of Oracle EBS patches, in all EBS instances, by an Oracle Apps DBA
Patching exceeding the contracted hours will be billed on a time and materials with prior written approval by the Client

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing

- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

Application Upgrades

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

600186 Oracle JDE application administration (CNC)

Company's Responsibilities and Included Features

Application Administration

Basic CNC Services:

- Monitor Enterprise One services
- Monitor disk space utilization
- Monitor UBE and other Enterprise One processes
- Monitor and review Enterprise One server logs and incident analysis

Advanced CNC Services:

- Environment and Path code maintenance, including data source and object configuration management
- Cloning environments - Up to one clone per month for each non-production instance or as specified in Line Item Service Boundaries *
- Data and path code refreshes, and environment constructions
- Functional environment troubleshooting and administration to cover Menus, data dictionary, object specifications, and OCM mappings
- Interactive and batch job monitoring and maintenance, to include troubleshooting and incident troubleshooting
- Job scheduler monitoring and scheduler server support
- OMW and Object configuration Management, to include project promotions, transfer rules, PVC administration
- Web forms, and application integrations, and task maintenance
- Default and direct/immediate printer management
- Infrastructure performance monitoring and tuning to support user and process growth
- Oracle Application Server maintenance

Custom object change management:

- Package builds and deployment of customizations through DV, PY, and other environments (as applicable) through to PD
- Object promotions to include version management and menu maintenance
- Change control of package builds, package management and deployments

24x7x365 Help desk support

* Requires a 5 business day notification for planning.

Incident Diagnosis and Troubleshooting

- Diagnosis of system incidents
- Troubleshooting of system incidents
- Engagement of Oracle support

Where necessary Company will engage and log service requests with Oracle to rectify software issues

- Provide client with updates

Document user issues and system errors

Patching and Upgrades

Application patching includes research and application of critical updates, recommended patches, legislative (Vertex, year-end) updates, and security patches

Break-Fix Patching - Break-Fix patch application will follow the incident priority response SLA

Enterprise One Break-Fix patching is defined as - A patch or series of patches required by Oracle to rectify an error in the application code of Oracle Enterprise One functionality that has already been implemented, tested and is in production in the Client's environment and include any individual ESUs, dependent ESU sets, required to addressed cuClientpecific Enterprise One application issues in functionality that has already been implemented, tested and is in production in the custClientvironment, and any Oracle recommended critical Patchset or Minipack needed to address known issues affecting a customClientronment

Non Break-Fix Patching - Non Break-Fix patching requires a 5 business day notification for planning.

- The following are types of patches which are not deemed to be Break-Fix:
- Enterprise One foundation enhancements
- Applications functional enhancements
- Planner ESUs and patch sets
- Enterprise One module and application implementations
- Enterprise One Service
- Prerequisite ESUs for third party application integrations
- Platform specific performance and tuning updates

Major Version Upgrades - Any major version upgrades, will be treated on a time and material basis and shall be planned and billed to Client as agreed upon by the Parties

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Application Security Administration

System security administration of the Enterprise One application:

- Enterprise User Management to include:
- user id creations
- group/role maintenance
- user override and mapping support

Enterprise One security workbench and strategy planning to support security planning and implementation, row, column, application, and solutions explorer security maintenance in consultation with Client functional analyst

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

600187 Oracle Business Intelligence Enterprise Edition application administration

Company's Responsibilities and Included Features

General

Oracle Business Intelligence Enterprise Edition (OBIEE) application administration is provided where OBIEE is used solely for reporting of Oracle EBS data

- Manage the following areas within the application:
- User security group/role maintenance within the application as defined by the Client
- Application monitoring
- Starting, stopping and restarting services.

24x7x365 Help desk support

Incident Triage and Resolution

Company will triage and manage the troubleshooting process for technical system errors.
Company will research problems and issues utilizing:

- Company knowledge of known errors and their solution
- General operating system level troubleshooting
- Escalation to software provider

Resolution of system incidents:

- Application of Company known solutions
- Application of software vendor provided solutions

Engagement of software providers Help Desk support
Document user issues and system errors

Patching and Upgrades

Standard Patch Maintenance - Company shall provide patch application where patches for the application are within the following criteria:

- One-off patches - Patch to address a specific failure to standard functionality (i.e. Break-Fix)
- Any single or group of patches (Service Pack) required to solve a single issue or required by software vendor
- The patching activity is not associated with an application version upgrade

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents

- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Development Support

Provide application development resources to develop new or modify existing configurations, extensions, modifications, localizations and integrations

- Develop technical specification based upon functional requirements
- Develop or modify application objects
- Develop or modify reports
- Conduct unit and integration testing
- Document customizations

Database Support

- Provide support for all underlying databases supporting the OBIEE application including all data source databases.
- Provide all data ETL design, implement and manage functions.

600219 Oracle Data Integrator Application Administration

Company's Responsibilities and Included Features

General

Oracle Data Integrator (ODI) application administration is provided where ODI is used solely for integration with Oracle EBS.

- Manage the following areas within the application:
- User security group/role maintenance within the application as defined by the Client
- Application monitoring
- Starting, stopping and restarting services.

24x7x365 Help desk support

Incident Triage and Troubleshooting

Company will triage and manage the troubleshooting process for technical system errors.
Company will research problems and issues utilizing:

- Company knowledge of known errors and their solution
- General operating system level troubleshooting

- Escalation to software provider

Troubleshooting of system incidents:

- Application of Company known solutions
- Application of software vendor provided solutions

Engagement of software providers Help Desk support
Document user issues and system errors

Patching and Upgrades

Standard Patch Maintenance - Company shall provide patch application where patches for the application are within the following criteria:

- One-off patches - Patch to address a specific failure to standard functionality (i.e. Break-Fix)
- Any single or group of patches (Service Pack) required to solve a single issue or required by software vendor
- The patching activity is not associated with an application version upgrade

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Development Support

Provide application development resources to develop new or modify existing configurations, extensions, modifications, localizations and integrations

- Develop technical specification based upon functional requirements
- Develop or modify application objects
- Develop or modify reports
- Conduct unit and integration testing

- Document customizations

Database Support

- Provide support for all underlying databases supporting the OBIEE application including all data source databases.
- Provide all data ETL design, implement and manage functions.

600220 Oracle SOA Suite Disaster Recovery Application Administration

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of an Oracle SOA environment in a recovery site acting as a failover environment.
Replication of the application binaries and file systems from the primary servers to the target DR servers is to be provided through the use of server to server replication software and requires an OS replication Service Item which will perform the replication.
Company shall develop and maintain Disaster Recovery Failover Procedures.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Application Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client
- The number of failover tests per year is referenced in Service Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster occur during a test the data will be as old as the data was when testing began.

Application Failover Services

On declaration of a disaster, Company will perform the steps necessary to restart and validate the application on the target DR server and make it the primary application environment, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
During the period that the target DR server is acting as the primary environment, administration of the Oracle SOA application will be as per the administrative, support, backup and monitoring services as defined for the primary environment.

Application Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The application administrator will assist the operating systems administrator reestablish application file system replication back to the target DR server.

Application Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Third Party Application Dependency Management

- Management of third party application interface to the application
- Administration of third party applications associated with this DR environment.

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

600221 Oracle Data Integrator Disaster Recovery Application Administration

Company's Responsibilities and Included Features

General

Company shall provide disaster recovery services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of an Oracle Data Integrator (ODI) environment in a recovery site acting as a failover environment.

Replication of the application binaries and file systems from the primary servers to the target DR servers is to be provided through the use of server to server replication software and requires an OS replication Service Item which will perform the replication.

Company shall develop and maintain Disaster Recovery Failover Procedures.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Application Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client
- The number of failover tests per year is referenced in Service Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster occur during a test the data will be as old as the data was when testing began.

Application Failover Services

On declaration of a disaster, Company will perform the steps necessary to restart and validate the application on the target DR server and make it the primary application environment, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.

During the period that the target DR server is acting as the primary environment, administration of the Oracle Data Integrator application will be as per the administrative, support, backup and monitoring services as defined for the primary environment.

Application Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The application administrator will assist the operating systems administrator reestablish application file system replication back to the target DR server.
- Application Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as

further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Third Party Application Dependency Management

- Management of third party application interface to the application
- Administration of third party applications associated with this DR environment.

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

600222 Oracle SOA Suite Application Administration

Company's Responsibilities and Included Features

General

Oracle SOA Suite application administration is provided where Oracle SOA Suite is used solely for integration to Oracle EBS.

- Manage the following areas within the application:
- User security group/role maintenance within the application as defined by the Client
- Application monitoring
- Starting, stopping and restarting services.

24x7x365 Help desk support

Incident Triage and Troubleshooting

Company will triage and manage the troubleshooting process for technical system errors.
Company will research problems and issues utilizing:

- Company knowledge of known errors and their solution
- General operating system level troubleshooting
- Escalation to software provider

Troubleshooting of system incidents:

- Application of Company known solutions
- Application of software vendor provided solutions

Engagement of software providers Help Desk support
Document user issues and system errors

Patching and Upgrades
Standard Patch Maintenance - Company shall provide patch application where patches for the application are within the following criteria:

- One-off patches - Patch to address a specific failure to standard functionality (i.e. Break-Fix)
- Any single or group of patches (Service Pack) required to solve a single issue or required by software vendor
- The patching activity is not associated with an application version upgrade

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)
End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Development Support
Provide application development resources to develop new or modify existing configurations, extensions, modifications, localizations and integrations

Develop technical specification based upon functional requirements

- Develop or modify application objects
- Develop or modify reports
- Conduct unit and integration testing
- Document customizations

Database Support

- Provide support for all underlying databases supporting the OBIEE application including all data source databases.
- Provide all data ETL design, implement and manage functions.

600449 Oracle EBS Financial, Procurement and Project Techno-Functional Support - Offshore

Company's Responsibilities and Included Features

Techno-Functional Support*

- Provide Techno-Functional (TF) support in the use of Oracle EBS to Client key end users in each of the following areas:
  - Financials
    - General Ledger (GL)
    - Accounts Payable (AP)
    - Accounts Receivables (AR)
    - Fixed Assets (FA)
    - Cash Management (CM)
    - i-Expense
    - Tax
  - Procure to Pay
    - iProcurement
    - Purchasing (PO)
    - iSupplier
  - Projects
    - Project Management
    - Project Costing
- Troubleshoot and diagnose functional incidents
- Perform Oracle patch impact analysis
- Support month-end close, benefits enrollment, payroll runs, and reporting
- Work with the business on day-day data fixes and consolidation process
- Perform root cause analysis (RCA) for critical and repetitive functional tickets
- Coordinate TF incidents with Company technical administration team and 3rd party vendors, including Oracle
- Communicate TF support status to leadership team
- Act as the Client liaison with software vendors for incident troubleshooting
- Participate in the functional design and testing of customizations to Oracle EBS, as defined by Client
- Functional Change Request (CR) management
  - Initiate, seek approval and execute functional change requests as per approval procedures.
  - Includes:
    - Configuration changes
    - Functional setups
    - Manage, review, execute urgent CR s
    - Follow change management procedures and document changes
- Participate in any additional TF projects or initiatives required by Client
- Company assumes that the information provided during TF discussions and through documents is accurate and up-to-date. Result of incorrect information can result in risk to business systems stability and data integrity and could result in support hours being consumed for rework
- Workaround(s) to production bugs will be suggested by OneNeck team only if they are supported by Oracle

- For any TF or development issues raised by Client, Company shall work each such issue for up to four (4) hours, upon reaching the four-hour limit for any one issue, Company shall contact Client to receive approval to continue the proposed troubleshooting
- Oracle CSR resolution is dependent on the solutions or fixes from Oracle Corporation
- Company assumes that the Client's business users will be available for any discussion required for problem troubleshooting and resolution and will be provide in a timely manner

TF support is provided by non-USA resident resources (offshore)

*** TF support is limited to the number of hours per month as contracted, based upon a rolling three (3) month average of hours consumed. Bursts in monthly consumption may not exceed 10% of contracted hours.**

TF Support Prioritization and Engagement Objectives

- Company will provide support to the Client s Oracle EBS users for TF support through question and issue submission through incident tickets submitted to and administered by Company s help desk, prioritized as follows:

Priority	Definition	Support Hours	Engagement Objective during Support Hours
1	One or more business critical application functions is impeding the customer s ability to perform business.	Monday-Friday, 6pm-12pm ET	30 minutes
2	One or more business critical application functions are degraded and is impacting the customer s ability to perform business.	Monday-Friday, 6pm-12pm ET	2 hours
3	The incident has a medium impact on the customer's ability to perform business.	Monday-Friday, 6pm-12pm ET	4 hours
4	The incident has a minor impact on the customer's ability to perform business.	Monday-Friday, 6pm-12pm ET	24 hours
5	The incident has no impact to the customer s ability to perform business.	Monday-Friday, 6pm-12pm ET	48 hours

- TF support will be provided on a best effort basis for any time outside of the designated support hours, unless agreed upon in advance by both parties

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Screening Functional Issues
  - Client shall internally review each functional issue and determine the necessity of escalating such issue to Company. This is done to limit unnecessary use of allocated functional support hours
- Oracle EBS Development
  - Code Development
  - Report Development
  - Code troubleshooting and maintenance
- Necessary software licensing to enable functional support staff to access Client systems

600450 Oracle EBS HRMS Techno-Functional Support - Offshore

Company's Responsibilities and Included Features

Techno-Functional Support*

- Provide Techno-Functional (TF) support in the use of Oracle EBS HRMS to Client key end users in each of the following areas:
  - Human Resources
    - HRMS
    - iRecruitment
    - Advanced Benefits
    - Payroll

        - iLearning Management
        - Time Entry
        - Performance Management

- Troubleshoot and diagnose functional incidents
- Perform Oracle patch impact analysis
- Support month-end close, benefits enrollment, payroll runs, and reporting
- Work with the business on day-day data fixes and consolidation process
- Perform root cause analysis (RCA) for critical and repetitive functional tickets
- Coordinate TF incidents with Company technical administration team and 3rd party vendors, including Oracle
- Communicate TF support status to leadership team
- Act as the Client liaison with software vendors for incident troubleshooting
- Participate in the functional design and testing of customizations to Oracle EBS HRMS, as defined by Client
- Functional Change Request (CR) management
    - Initiate, seek approval and execute functional change requests as per approval procedures.
    - Includes:
        - Configuration changes
        - Functional setups
        - Manage, review, execute urgent CR s
        - Follow change management procedures and document changes
- Participate in any additional TF projects or initiatives required by Client
- Company assumes that the information provided during TF discussions and through documents is accurate and up-to-date. Result of incorrect information can result in risk to business systems stability and data integrity and could result in support hours being consumed for rework
- Workaround(s) to production bugs will be suggested by OneNeck team only if they are supported by Oracle
- For any TF or development issues raised by Client, Company shall work each such issue for up to four (4) hours, upon reaching the four-hour limit for any one issue, Company shall contact Client to receive approval to continue the proposed troubleshooting
- Oracle CSR resolution is dependent on the solutions or fixes from Oracle Corporation
- Company assumes that the Client's business users will be available for any discussion required for problem troubleshooting and resolution and will be provide in a timely manner

TF support is provided by non-USA resident resources (offshore)

*** TF support is limited to the number of hours per month as contracted, based upon a rolling three (3) month average of hours consumed. Bursts in monthly consumption may not exceed 10% of contracted hours.**

TF Support Prioritization and Engagement Objectives

- Company will provide support to the Client s Oracle EBS HRMS users for TF support through question and issue submission through incident tickets submitted to and administered by Company s help desk, prioritized as follows:

Priority	Definition	Support Hours	Engagement Objective during Support Hours
1	One or more business critical application functions is impeding the customer s ability to perform business.	Monday-Friday, 6pm-12pm ET	30 minutes
2	One or more business critical application functions are degraded and is impacting the customer s ability to perform business.	Monday-Friday, 6pm-12pm ET	2 hours
3	The incident has a medium impact on the customer's ability to perform business.	Monday-Friday, 6pm-12pm ET	4 hours
4	The incident has a minor impact on the customer's ability to perform business.	Monday-Friday, 6pm-12pm ET	24 hours
5	The incident has no impact to the customer s ability to perform business.	Monday-Friday, 6pm-12pm ET	48 hours

- TF support will be provided on a best effort basis for any time outside of the designated support hours, unless agreed

upon in advance by both parties

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Screening Functional Issues
  - Client shall internally review each functional issue and determine the necessity of escalating such issue to Company. This is done to limit unnecessary use of allocated functional support hours
- Oracle EBS HRMS Development
  - Code Development
  - Report Development
  - Code troubleshooting and maintenance
- Necessary software licensing to enable functional support staff to access Client systems

600451 Oracle EBS Financial, Procurement and Project Development Support - Offshore

Company's Responsibilities and Included Features

Development Support Module Scope

- Provide development support within each of the following areas of Oracle EBS:
  - Financials
    - General Ledger (GL)
    - Accounts Payable (AP)
    - Accounts Receivables (AR)
    - Fixed Assets (FA)
    - Cash Management (CM)
    - i-Expense
    - Tax
  - Procure to Pay
    - iProcurement
    - Purchasing (PO)
    - iSupplier
  - Projects
    - Project Management
    - Project Costing

Development support is provided by non-USA resident resources (offshore)

Development support is limited to the number of hours per month as contracted, based upon a rolling three (3) month average of hours consumed. Bursts in monthly consumption may not exceed 10% of contracted hours.

Configuration, Extension, Modification, Localization, and Integration (CEMLI) Development and Support

- Provide Oracle EBS Development resources to modify existing configurations, extensions, modifications, localizations and integrations including:
  - Technical specification documentation
  - Technical design
  - Document CEMLI object development
  - Development, coding, modify application objects
  - Conduct unit and integration testing with assistance from functional personnel
  - Technical issue support
  - Performance issue support
  - Third party integration configuration and trouble shooting
  - Workflow / Concurrent Manager issue support
  - Providing support with transaction processing issues
  - Support OAF / Forms / Reports
- Follow promotions, change management and governance as per Client's policies and procedures

Participate in and conduct peer code and deliverable reviews
- Coordinate with functional team for user acceptance testing and approval to migrate to production
- Update the relevant documents in the change management system
- Once a CEMLI is identified for break-fix or development, the following process will be followed:
    - Company support lead will finalize a development resource consumption estimate and provide a delivery date. Changes in priorities as defined by the Client can affect delivery dates, before and after commencement of development work.
    - Development will commence once Client approves the estimates and dates
    - Actual delivery dates will be tracked and reported to Client
    - Quarterly compliance of promised to actual delivery date will be monitored and communicated to Client
    - A list of CEMLI's with the priority, start date, completion date, test date and closure date will be maintained and discussed in the weekly call with the Client.

CEMLI Maintenance

- Provide Oracle EBS Development support for existing CEMLI:
    - Troubleshooting and rectification of CEMLI failures and problems where configuration or coding errors are found
    - Assist functional personnel with application data repair
    - Assist technical personnel with application patch research

Development Support Prioritization and Engagement Objectives

- Company will provide development support to the Client s Oracle EBS environments through request, question and issue submission through incident tickets submitted to and administered by Company s help desk, prioritized as follows:

Priority	Definition	Support Hours	Engagement Objective during Support Hours
1	One or more business critical application functions is impeding the customer s ability to perform business.	Monday-Friday, 6pm-12pm ET	30 minutes
2	One or more business critical application functions are degraded and is impacting the customer s ability to perform business.	Monday-Friday, 6pm-12pm ET	2 hours
3	The incident has a medium impact on the customer's ability to perform business.	Monday-Friday, 6pm-12pm ET	4 hours
4	The incident has a minor impact on the customer's ability to perform business.	Monday-Friday, 6pm-12pm ET	24 hours
5	The incident has no impact to the customer s ability to perform business.	Monday-Friday, 6pm-12pm ET	48 hours

- Development support will be provided on a best effort basis for any time outside of the designated support hours, unless agreed upon in advance by both parties

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Development Environment

- Provide development environment
- Provide remote access to development environment
- Necessary software licensing to enable development staff to access Client systems

600452 Oracle EBS HRMS Development Support - Offshore

Company's Responsibilities and Included Features

Development Support Module Scope

- Provide development support within each of the following areas of Oracle EBS HRMS:

- Human Resources
    - HRMS
    - iRecruitment
    - Advanced Benefits
    - Payroll
    - iLearning Management
    - Time Entry
    - Performance Management

Development support is provided by non-USA resident resources (offshore)

Development support is limited to the number of hours per month as contracted, based upon a rolling three (3) month average of hours consumed. Bursts in monthly consumption may not exceed 10% of contracted hours.

Configuration, Extension, Modification, Localization, and Integration (CEMLI) Development and Support

- Provide Oracle EBS HRMS Development resources to modify existing configurations, extensions, modifications, localizations and integrations including:
    - Technical specification documentation
    - Technical design
    - Document CEMLI object development
    - Development, coding, modify application objects
    - Conduct unit and integration testing with assistance from functional personnel
    - Technical issue support
    - Performance issue support
    - Third party integration configuration and trouble shooting
    - Workflow / Concurrent Manager issue support
    - Providing support with transaction processing issues
    - Support OAF / forms / reports
- Follow promotions, change management and governance as per Client's policy and procedures
- Participate in and conduct peer code and deliverable reviews
- Coordinate with functional team for user acceptance testing and approval to migrate to production
- Update the relevant documents in the change management system
- Once a CEMLI is identified for break-fix or development, the following process will be followed:
    - Company support lead will finalize a development resource consumption estimate and provide a delivery date. Changes in priorities as defined by the Client can affect delivery dates, before and after commencement of development work.
    - Development will commence once Client approves the estimates and dates
    - Actual delivery dates will be tracked and reported to Client
    - Quarterly compliance of promised to actual delivery date will be monitored and communicated to Client
    - A list of CEMLI's with the priority, start date, completion date, test date and closure date will be maintained and discussed in the weekly call with the Client.

CEMLI Maintenance

- Provide Oracle EBS HRMS Development support for existing CEMLI:
    - Troubleshooting and rectification of CEMLI failures and problems where configuration or coding errors are found
    - Assist functional personnel with application data repair
    - Assist technical personnel with application patch research

Development Support Prioritization and Engagement Objectives

- Company will provide development support to the Client s Oracle HRMS environments through request, question and issue submission through incident tickets submitted to and administered by Company s help desk, prioritized as follows:

Priority	Definition	Support Hours	Engagement Objective during Support Hours

1	One or more business critical application functions is impeding the customer s ability to perform business.	Monday-Friday, 6pm-12pm ET	30 minutes
2	One or more business critical application functions are degraded and is impacting the customer s ability to perform business.	Monday-Friday, 6pm-12pm ET	2 hours
3	The incident has a medium impact on the customer's ability to perform business.	Monday-Friday, 6pm-12pm ET	4 hours
4	The incident has a minor impact on the customer's ability to perform business.	Monday-Friday, 6pm-12pm ET	24 hours
5	The incident has no impact to the customer s ability to perform business.	Monday-Friday, 6pm-12pm ET	48 hours

- Development support will be provided on a best effort basis for any time outside of the designated support hours, unless agreed upon in advance by both parties

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Development Environment

- Provide development environment
- Provide remote access to development environment
- Necessary software licensing to enable development staff to access Client systems

600453 Oracle EBS Financial, Procurement and Project Techno-Functional Support - Onshore

Company's Responsibilities and Included Features

Techno-Functional Support*

- Provide Techno-Functional (TF) support in the use of Oracle EBS to Client key end users in each of the following areas:
  - Financials
    - General Ledger (GL)
    - Accounts Payable (AP)
    - Accounts Receivables (AR)
    - Fixed Assets (FA)
    - Cash Management (CM)
    - i-Expense
    - Tax
  - Procure to Pay
    - iProcurement
    - Purchasing (PO)
    - iSupplier
  - Projects
    - Project Management
    - Project Costing
- Troubleshoot and diagnose functional incidents
- Perform Oracle patch impact analysis
- Support month-end close, benefits enrollment, payroll runs, and reporting
- Work with the business on day-day data fixes and consolidation process
- Perform root cause analysis (RCA) for critical and repetitive functional tickets
- Coordinate TF incidents with Company technical administration team and 3rd party vendors, including Oracle
- Communicate TF support status to leadership team
- Act as the Client liaison with software vendors for incident troubleshooting
- Participate in the functional design and testing of customizations to Oracle EBS, as defined by Client
- Functional Change Request (CR) management

        - Initiate, seek approval and execute functional change requests as per approval procedures.
        - Includes:
            - Configuration changes
            - Functional setups
            - Manage, review, execute urgent CR s
            - Follow change management procedures and document changes
    - Participate in any additional TF projects or initiatives required by Client
    - Company assumes that the information provided during TF discussions and through documents is accurate and up-to-date. Result of incorrect information can result in risk to business systems stability and data integrity and could result in support hours being consumed for rework
    - Workaround(s) to production bugs will be suggested by OneNeck team only if they are supported by Oracle
    - For any TF or development issues raised by Client, Company shall work each such issue for up to four (4) hours, upon reaching the four-hour limit for any one issue, Company shall contact Client to receive approval to continue the proposed troubleshooting
    - Oracle CSR resolution is dependent on the solutions or fixes from Oracle Corporation
    - Company assumes that the Client's business users will be available for any discussion required for problem troubleshooting and resolution and will be provided in a timely manner

TF support is provided by USA resident resources (onshore)

*** TF support is limited to the number of hours per month as contracted, based upon a rolling three (3) month average of hours consumed. Bursts in monthly consumption may not exceed 10% of contracted hours.**

TF Support Prioritization and Engagement Objectives

- Company will provide support to the Client s Oracle EBS users for TF support through question and issue submission through incident tickets submitted to and administered by Company s help desk, prioritized as follows:

Priority	Definition	Support Hours	Engagement Objective during Support Hours
1	One or more business critical application functions is impeding the customer s ability to perform business.	Monday-Friday, 9am-6pm ET	30 minutes
2	One or more business critical application functions are degraded and is impacting the customer s ability to perform business.	Monday-Friday, 9am-6pm ET	2 hours
3	The incident has a medium impact on the customer's ability to perform business.	Monday-Friday, 9am-6pm ET	4 hours
4	The incident has a minor impact on the customer's ability to perform business.	Monday-Friday, 9am-6pm ET	24 hours
5	The incident has no impact to the customer s ability to perform business.	Monday-Friday, 9am-6pm ET	48 hours

- TF support will be provided on a best effort basis for any time outside of the designated support hours, unless agreed upon in advance by both parties

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Screening Functional Issues
    - Client shall internally review each functional issue and determine the necessity of escalating such issue to Company. This is done to limit unnecessary use of allocated functional support hours
- Oracle EBS Development
    - Code Development
    - Report Development
    - Code troubleshooting and maintenance
- Necessary software licensing to enable functional support staff to access Client systems

600454 Oracle EBS HRMS Techno-Functional Support - Onshore

Company's Responsibilities and Included Features

Techno-Functional Support*

- Provide Techno-Functional (TF) support in the use of Oracle EBS HRMS to Client key end users in each of the following areas:
    - Human Resources
        - HRMS
        - iRecruitment
        - Advanced Benefits
        - Payroll
        - iLearning Management
        - Time Entry
        - Performance Management
- Troubleshoot and diagnose functional incidents
- Perform Oracle patch impact analysis
- Support month-end close, benefits enrollment, payroll runs, and reporting
- Work with the business on day-day data fixes and consolidation process
- Perform root cause analysis (RCA) for critical and repetitive functional tickets
- Coordinate TF incidents with Company technical administration team and 3rd party vendors, including Oracle
- Communicate TF support status to leadership team
- Act as the Client liaison with software vendors for incident troubleshooting
- Participate in the functional design and testing of customizations to Oracle EBS, as defined by Client
- Functional Change Request (CR) management
    - Initiate, seek approval and execute functional change requests as per approval procedures.
    - Includes:
        - Configuration changes
        - Functional setups
        - Manage, review, execute urgent CR s
        - Follow change management procedures and document changes
- Participate in any additional TF projects or initiatives required by Client
- Company assumes that the information provided during TF discussions and through documents is accurate and up-to-date. Result of incorrect information can result in risk to business systems stability and data integrity and could result in support hours being consumed for rework
- Workaround(s) to production bugs will be suggested by OneNeck team only if they are supported by Oracle
- For any TF or development issues raised by Client, Company shall work each such issue for up to four (4) hours, upon reaching the four-hour limit for any one issue, Company shall contact Client to receive approval to continue the proposed troubleshooting
- Oracle CSR resolution is dependent on the solutions or fixes from Oracle Corporation
- Company assumes that the Client's business users will be available for any discussion required for problem troubleshooting and resolution and will be provide in a timely manner

TF support is provided by USA resident resources (onshore)

*** TF support is limited to the number of hours per month as contracted, based upon a rolling three (3) month average of hours consumed. Bursts in monthly consumption may not exceed 10% of contracted hours.**

TF Support Prioritization and Engagement Objectives

- Company will provide support to the Client s Oracle EBS HRMS users for TF support through question and issue submission through incident tickets submitted to and administered by Company s help desk, prioritized as follows:

Priority	Definition	Support Hours	Engagement Objective during Support Hours
1	One or more business critical application functions is impeding the customer s ability to perform business.	Monday-Friday, 9am-6pm ET	30 minutes

2	One or more business critical application functions are degraded and is impacting the customer s ability to perform business.	Monday-Friday, 9am-6pm ET	2 hours
3	The incident has a medium impact on the customer's ability to perform business.	Monday-Friday, 9am-6pm ET	4 hours
4	The incident has a minor impact on the customer's ability to perform business.	Monday-Friday, 9am-6pm ET	24 hours
5	The incident has no impact to the customer s ability to perform business.	Monday-Friday, 9am-6pm ET	48 hours

- TF support will be provided on a best effort basis for any time outside of the designated support hours, unless agreed upon in advance by both parties

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Screening Functional Issues
  - Client shall internally review each functional issue and determine the necessity of escalating such issue to Company. This is done to limit unnecessary use of allocated functional support hours
- Oracle EBS HRMS Development
  - Code Development
  - Report Development
  - Code troubleshooting and maintenance
- Necessary software licensing to enable functional support staff to access Client systems

600455 Oracle EBS Financial, Procurement and Project Development Support - Onshore

Company's Responsibilities and Included Features

Development Support Module Scope

- Provide development support within each of the following areas of Oracle EBS:
  - Financials
    - General Ledger (GL)
    - Accounts Payable (AP)
    - Accounts Receivables (AR)
    - Fixed Assets (FA)
    - Cash Management (CM)
    - i-Expense
    - Tax
  - Procure to Pay
    - iProcurement
    - Purchasing (PO)
    - iSupplier
  - Projects
    - Project Management
    - Project Costing

Development support is provided by USA resident resources (onshore)

Development support is limited to the number of hours per month as contracted, based upon a rolling three (3) month average of hours consumed. Bursts in monthly consumption may not exceed 10% of contracted hours.

Configuration, Extension, Modification, Localization, and Integration (CEMLI) Development and Support

- Provide Oracle EBS Development resources to modify existing configurations, extensions, modifications, localizations and integrations including:
  - Technical specification documentation
  - Technical design

        - Document CEMLI object development
        - Development, coding, modify application objects
        - Conduct unit and integration testing with assistance from functional personnel
        - Technical issue support
        - Performance issue support
        - Third party integration configuration and trouble shooting
        - Workflow / Concurrent Manager issue support
        - Providing support with transaction processing issues
        - Support OAF / Forms / Reports
    - Follow promotions, change management and governance as per Client's policy and procedures
    - Participate in and conduct peer code and deliverable reviews
    - Coordinate with functional team for user acceptance testing and approval to migrate to production
    - Update the relevant documents in the change management system
    - Once a CEMLI is identified for break-fix or development, the following process will be followed:
        - Company support lead will finalize a development resource consumption estimate and provide a delivery date. Changes in priorities as defined by the Client can affect delivery dates, before and after commencement of development work.
        - Development will commence once Client approves the estimates and dates
        - Actual delivery dates will be tracked and reported to Client
        - Quarterly compliance of promised to actual delivery date will be monitored and communicated to Client
        - A list of CEMLI's with the priority, start date, completion date, test date and closure date will be maintained and discussed in the weekly call with the Client.

CEMLI Maintenance

- Provide Oracle EBS Development support for existing CEMLI:
    - Troubleshooting and rectification of CEMLI failures and problems where configuration or coding errors are found
    - Assist functional personnel with application data repair
    - Assist technical personnel with application patch research

Development Support Prioritization and Engagement Objectives

- Company will provide development support to the Client s Oracle EBS environments through request, question and issue submission through incident tickets submitted to and administered by Company s help desk, prioritized as follows:

Priority	Definition	Support Hours	Engagement Objective during Support Hours
1	One or more business critical application functions is impeding the customer s ability to perform business.	Monday-Friday, 9am-6pm ET	30 minutes
2	One or more business critical application functions are degraded and is impacting the customer s ability to perform business.	Monday-Friday, 9am-6pm ET	2 hours
3	The incident has a medium impact on the customer's ability to perform business.	Monday-Friday, 9am-6pm ET	4 hours
4	The incident has a minor impact on the customer's ability to perform business.	Monday-Friday, 9am-6pm ET	24 hours
5	The incident has no impact to the customer s ability to perform business.	Monday-Friday, 9am-6pm ET	48 hours

- Development support will be provided on a best effort basis for any time outside of the designated support hours, unless agreed upon in advance by both parties

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Development Environment

- Provide development environment
- Provide remote access to development environment
- Necessary software licensing to enable development staff to access Client systems

600456 Oracle EBS HRMS Development Support - Onshore

Company's Responsibilities and Included Features

Development Support Module Scope

- Provide development support within each of the following areas of Oracle EBS HRMS:
  - Human Resources
    - HRMS
    - iRecruitment
    - Advanced Benefits
    - Payroll
    - iLearning Management
    - Time Entry
    - Performance Management

Development support is provided by USA resident resources (onshore)

Development support is limited to the number of hours per month as contracted, based upon a rolling three (3) month average of hours consumed. Bursts in monthly consumption may not exceed 10% of contracted hours.

Configuration, Extension, Modification, Localization, and Integration (CEMLI) Development and Support

- Provide Oracle EBS HRMS Development resources to modify existing configurations, extensions, modifications, localizations and integrations including:
  - Technical specification documentation
  - Technical design
  - Document CEMLI object development
  - Development, coding, modify application objects
  - Conduct unit and integration testing with assistance from functional personnel
  - Technical issue support
  - Performance issue support
  - Third party integration configuration and trouble shooting
  - Workflow / Concurrent Manager issue support
  - Providing support with transaction processing issues
  - Support OAF / Forms / Reports
- Follow promotions, change management and governance as per Client's policies and procedures
- Participate in and conduct peer code and deliverable reviews
- Coordinate with functional team for user acceptance testing and approval to migrate to production
- Update the relevant documents in the change management system
- Once a CEMLI is identified for break-fix or development, the following process will be followed:
  - Company support lead will finalize a development resource consumption estimate and provide a delivery date. Changes in priorities as defined by the Client can affect delivery dates, before and after commencement of development work.
  - Development will commence once Client approves the estimates and dates
  - Actual delivery dates will be tracked and reported to Client
  - Quarterly compliance of promised to actual delivery date will be monitored and communicated to Client
  - A list of CEMLI's with the priority, start date, completion date, test date and closure date will be maintained and discussed in the weekly call with the Client.

CEMLI Maintenance

- Provide Oracle EBS HRMS Development support for existing CEMLI:
  - Troubleshooting and rectification of CEMLI failures and problems where configuration or coding errors are found
  - Assist functional personnel with application data repair
  - Assist technical personnel with application patch research

Development Support Prioritization and Engagement Objectives

- Company will provide development support to the Client s Oracle EBS HRMS environments through request, question and issue submission through incident tickets submitted to and administered by Company s help desk, prioritized as follows:

Priority	Definition	Support Hours	Engagement Objective during Support Hours
1	One or more business critical application functions is impeding the customer s ability to perform business.	Monday-Friday, 9am-6pm ET	30 minutes
2	One or more business critical application functions are degraded and is impacting the customer s ability to perform business.	Monday-Friday, 9am-6pm ET	2 hours
3	The incident has a medium impact on the customer's ability to perform business.	Monday-Friday, 9am-6pm ET	4 hours
4	The incident has a minor impact on the customer's ability to perform business.	Monday-Friday, 9am-6pm ET	24 hours
5	The incident has no impact to the customer s ability to perform business.	Monday-Friday, 9am-6pm ET	48 hours

- Development support will be provided on a best effort basis for any time outside of the designated support hours, unless agreed upon in advance by both parties

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Development Environment

- Provide development environment
- Provide remote access to development environment
- Necessary software licensing to enable development staff to access Client systems

600465 Oracle EBS Minor Release Upgrade

Company's Responsibilities and Included Features

Services Overview

- Company will provide one upgrade per contract year of the Client s Oracle EBS Application to the mutually agreed minor version Oracle EBS (..X) and apply the mutually agreed HRMS Release Update Patch (RUP), as well as any other mutually agreed RUPs. Each module may only have one RUP applied during the contract year and must be accomplished during and as part of the upgrade project.
- The upgrade will be limited to upgrading 4 Oracle EBS environments as listed:
  - Development (Development/sandbox)
  - Test (Unit/integration testing)
  - UAT (Business testing)
  - Production
- Company will be responsible for the following aspects of the upgrade:
  - Project management
  - Functional review of module impacts based upon version release notes
  - Technical and dependent patch analysis
  - Analysis of CEMLI impact

    - Retrofit necessary existing CEMLI
    - Supporting Client functional teams in updating and developing test plans
    - Supporting Client functional teams in testing
    - Preparing minor version and RUP upgrade apply plans for each environment
    - Technical upgrade and application of RUPs to each environment
    - Recommending and applying EBS functional configuration changes
- This service will be billed as a monthly fee

Project Oversight

Company will assign a Project Manager (PM) to act as a single point of contact for the project, perform project oversight, and provide status reporting for this service. Specifically, the Company PM will:

- Assemble Resources. The PM will assemble required Company resources necessary to deliver the Services.
- Schedule a Project Kick-Off Meeting. The PM will schedule a kick-off meeting with Company project resources and Client project resources to review the scope of services and discuss scheduled activities.
- Develop a Project Plan. The PM will develop and maintain a project plan incorporating the overall schedule for delivery of services including dependencies, task assignments, and milestones.
- Provide Communications. The PM will manage overall project communications per an agreed upon communications plan.
- Perform Risk and Issue Management. The PM will manage and document all risks and issues associated with the services and communicate as needed with the Client.
- Coordinate Activities. The PM will coordinate and schedule all activities associated with the services, including meetings, change windows, and engineering activities.
- Monitor Progress. The PM will monitor progress of the services and escalate and provide mitigation plans for related issues.
- Control Scope and Budget. The PM will control the defined scope of services and stay within the defined budget. Any changes to scope or budget will be documented and agreed to in a change order submitted to the Client for approval.
- Close out Project. The PM will confirm Client s acceptance of all services and deliverables and close out the project.

Availability of Company Services

- Except as outlined below, Company personnel will provide the services to Client Monday through Friday, 8:00 AM to 5:00 PM local time based on the Company resource s work location (Normal Business Hours), excluding holidays recognized by Company.
- Integration and migration cutover events included in the upgrade project may be scheduled outside of Normal Business Hours by mutual agreement of the parties.

Deliverables

Company will provide the deliverables listed below in Company s standard format.

- Upgraded Oracle EBS as per Oracle EBS environments listed above.
- RUPs applied to HRMS and other necessary modules as identified and agreed upon during the project.
- Updated documentation on environments.
- Transition to operational support.
- End users training (train the trainer) resulting from any new or modified features or functions in the upgraded/patched environment.

Assumptions

- Usage of Company's techno-functional and development resources.
- To leverage the most current knowledge of the solution, Company expects to leverage up to 30% of the techno-functional and development resources from currently contracted team providing techno-functional and development support to Client.
- The upgrade process will be limited to making 3 clones of environments.
- Any non-Oracle EBS applications that may need to be upgraded because of the Oracle EBS upgrade are not included in

the scope of this service and will need to be contracted under a separate statement of work.

- Any upgrade of the Oracle databases used by the EBS applications that may need to be upgraded because of the Oracle EBS upgrade are not included in the scope of this service and will need to be contracted under a separate statement of work.
- Company requires four (4) weeks notice prior to starting the upgrade planning and execution.
- The upgrade needs to have been completed within the period of the contract.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Company s performance is dependent upon Client managing and fulfilling its responsibilities, including providing Company with the information and access it requires to perform the Services. Any delay in Client s performance of its responsibilities may result in additional charges and/or delay of the completion of the Services.
- Client will be responsible for the functional and technical testing/validation during each phase of the project.

Assumptions

- Additional infrastructure resources, e.g. compute, disk, etc. may be required and will be requested under additional statements of work.
- Client will manage the demand for techno-functional and development work during the upgrade project to free up the techno-functional and development resources for up to 30% of their contracted time to participate in the upgrade project.

600617 Oracle EBS Techno-Functional Support - Offshore

Company's Responsibilities and Included Features

Techno-Functional Support*

- Provide Techno-Functional (TF) support in the use of Oracle EBS to Client key end users in each of the following areas:
  - Supply Chain
    - Order Management
    - Quote
    - Advanced Pricing
    - iStore
    - Inventory
    - Bill of Materials
    - Work in Process
    - Engineering
  - Financials
    - General Ledger (GL)
    - Accounts Payable (AP)
    - Accounts Receivables (AR)
    - Advanced Collections
    - Fixed Assets (FA)
    - Cash Management (CM)
    - i-Expense
    - Tax
  - Procure to Pay
    - Purchasing (PO)
    - iSupplier
  - Projects
    - Project Billing
    - Project Costing
- Troubleshoot and diagnose functional incidents
- Perform Oracle patch impact analysis

- Support month-end close, transaction runs and reporting
- Work with the business on day-day data fixes and consolidation process
- Perform root cause analysis (RCA) for critical and repetitive functional tickets
- Coordinate TF incidents with Company technical administration team and 3rd party vendors, including Oracle and Rimini Street
- Communicate TF support status to leadership team
- Act as the Client liaison with software vendors for incident troubleshooting
- Participate in the functional design and testing of customizations to Oracle EBS, as defined by Client
- Functional Change Request (CR) management
    - Initiate, seek approval and execute functional change requests as per approval procedures.
    - Includes:
        - Configuration changes
        - Functional setups
        - Manage, review, execute urgent CR s
        - Follow change management procedures and document changes
- Participate in any additional TF projects or initiatives required by Client
- Company assumes that the information provided during TF discussions and through documents is accurate and up-to-date. Result of incorrect information can result in risk to business systems stability and data integrity and could result in support hours being consumed for rework
- Workaround(s) to production bugs will be suggested by OneNeck team only if they are supported by Oracle
- For any TF or development issues raised by Client, Company shall work each such issue for up to four (4) hours, upon reaching the four-hour limit for any one issue, Company shall contact Client to receive approval to continue the proposed troubleshooting
- Oracle CSR resolution is dependent on the solutions or fixes from Oracle Corporation
- Company assumes that the Client's business users will be available for any discussion required for problem troubleshooting and resolution and will be provide in a timely manner
- All incidents and requests will be logged and managed through Client provided incident management system

TF support is provided by non-USA resident resources (offshore)

*** TF support is limited to the number of hours per month as contracted, based upon a rolling three (3) month average of hours consumed. Bursts in monthly consumption may not exceed 10% of contracted hours.**

TF Support Prioritization and Engagement Objectives

- Company will provide support to the Client s Oracle EBS users for TF support through question and issue submission through incident tickets submitted to and administered by Company s help desk, prioritized as follows:

Priority	Definition	Support Hours	Engagement Objective during Support Hours
1	One or more business critical application functions is impeding the customer s ability to perform business.	Monday-Friday, 6pm-12pm CDT	30 minutes
2	One or more business critical application functions are degraded and is impacting the customer s ability to perform business.	Monday-Friday, 6pm-12pm CDT	2 hours
3	The incident has a medium impact on the customer's ability to perform business.	Monday-Friday, 6pm-12pm CDT	4 hours
4	The incident has a minor impact on the customer's ability to perform business.	Monday-Friday, 6pm-12pm CDT	24 hours
5	The incident has no impact to the customer s ability to perform business.	Monday-Friday, 6pm-12pm CDT	48 hours

- TF support will be provided on a best effort basis for any time outside of the designated support hours, unless agreed upon in advance by both parties

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Screening Functional Issues

        - Client shall internally review each functional issue and determine the necessity of escalating such issue to Company. This is done to limit unnecessary use of allocated functional support hours
    - Oracle EBS Development
        - Code Development
        - Report Development
        - Code troubleshooting and maintenance
    - Necessary software licensing to enable functional support staff to access Client systems

600619 Oracle EBS Techno-Functional Support Lead - Onshore

Company's Responsibilities and Included Features

Techno-Functional Support*

- Provide Techno-Functional (TF) support in the use of Oracle EBS to Client key end users in each of the following areas:
    - Supply Chain
        - Order Management
        - Quote
        - Advanced Pricing
        - iStore
        - Inventory
        - Bill of Materials
        - Work in Process

600620 Oracle EBS Development Support - Offshore

Company's Responsibilities and Included Features

Development Support Module Scope

- Provide development support within each of the following areas of Oracle EBS:
    - Supply Chain
        - Order Management
        - Quote
        - Advanced Pricing
        - iStore
        - Inventory
        - Bill of Materials
        - Work in Process
        - Engineering
    - Financials
        - General Ledger (GL)
        - Accounts Payable (AP)
        - Accounts Receivables (AR)
        - Advanced Collections
        - Fixed Assets (FA)
        - Cash Management (CM)
        - i-Expense
        - Tax
    - Procure to Pay
        - Purchasing (PO)
        - iSupplier
    - Projects
        - Project Billing
        - Project Costing

Development support is provided by non-USA resident resources (offshore)

Development support is limited to the number of hours per month as contracted, based upon a rolling three (3) month average of hours consumed. Bursts in monthly consumption may not exceed 10% of contracted hours.

Configuration, Extension, Modification, Localization, and Integration (CEMLI) Development and Support

- Provide Oracle EBS Development resources to modify existing configurations, extensions, modifications, localizations and integrations including:
  - Document CEMLI object development
  - Development, coding, modify application objects
  - Conduct unit and integration testing with assistance from functional personnel
  - Technical issue support
  - Performance issue support
  - Third party integration configuration and trouble shooting
  - Workflow / Concurrent Manager issue support
  - Providing support with transaction processing issues
  - Support OAF / Forms / Reports
- Follow promotions, change management and governance as per Client's policy and procedures
- Participate in and conduct peer code and deliverable reviews
- Coordinate with functional team for user acceptance testing and approval to migrate to production
- Update the relevant documents in the change management system
- All incidents and requests will be logged and managed through Client provided incident management system
- Once a CEMLI is identified for break-fix or development, the following process will be followed:
  - Company support lead will finalize a development resource consumption estimate and provide a delivery date. Changes in priorities as defined by the Client can affect delivery dates, before and after commencement of development work.
  - Development will commence once Client approves the estimates and dates
  - Actual delivery dates will be tracked and reported to Client
  - Quarterly compliance of promised to actual delivery date will be monitored and communicated to Client
  - A list of CEMLI's with the priority, start date, completion date, test date and closure date will be maintained and discussed in the weekly call with the Client.

CEMLI Maintenance

- Provide Oracle EBS Development support for existing CEMLI:
  - Troubleshooting and rectification of CEMLI failures and problems where configuration or coding errors are found
  - Assist functional personnel with application data repair
  - Assist technical personnel with application patch research

Development Support Prioritization and Engagement Objectives

- Company will provide development support to the Client s Oracle EBS environments through request, question and issue submission through incident tickets submitted to and administered by Company s help desk, prioritized as follows:

Priority	Definition	Support Hours	Engagement Objective during Support Hours
1	One or more business critical application functions is impeding the customer s ability to perform business.	Monday-Friday, 6pm-12pm CDT	30 minutes
2	One or more business critical application functions are degraded and is impacting the customer s ability to perform business.	Monday-Friday, 6pm-12pm CDT	2 hours
3	The incident has a medium impact on the customer's ability to perform business.	Monday-Friday, 6pm-12pm CDT	4 hours
	The incident has a minor impact on the customer's ability to	Monday-Friday,	

4	perform business.	6pm-12pm CDT	24 hours
5	The incident has no impact to the customer s ability to perform business.	Monday-Friday, 6pm-12pm CDT	48 hours

- Development support will be provided on a best effort basis for any time outside of the designated support hours, unless agreed upon in advance by both parties

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Development Environment

- Provide development environment
- Provide remote access to development environment
- Necessary software licensing to enable development staff to access Client systems

600621 Oracle EBS Support Management

Company's Responsibilities and Included Features

Oracle EBS Support Management*

* Oracle Support management is limited to number of hours per month as contracted.

Company will provide the following management services in support of the associated Oracle EBS Techno-Functional (TF) and development support contracted by Client with the Company:

- Provide qualified resource that has sufficient experience to enable effective understanding and ability to manage Oracle EBS technical and functional support teams and the associated incidents
- Perform Incidents analysis and heat map
- Manage day to day operations within the Oracle EBS support team including escalations
- Work with the business on process improvements
- Perform root cause analysis (RCA) for critical and repetitive functional tickets
- Coordinate TF incidents with Company technical administration team and 3rd party vendors, including Oracle and Rimini Street
- Communicate TF support status to Client leadership team
- Act as the Client liaison with software vendors for incident troubleshooting
- Coordinate Change Request (CR) management with customer teams
- Participate in any additional TF projects or initiatives required by Client
- Provide overall team management

Service Delivery

- Services will be available 9:00am to 5:00pm CDT Monday to Friday excluding Company holidays
- All incidents and requests will be logged and managed through Client provided incident management system
- Unconsumed hours for the month will not roll over to the next month

TF support is provided by USA resident resources (onshore)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

None

601451

Company's Responsibilities and Included Features

Techno-Functional Support*

- Provide Techno-Functional (TF) support in the use of Oracle EBS to Client key end-users in each of the following areas:
    - Financials
        - General Ledger (GL)
        - Accounts Payable (AP)
        - Accounts Receivables (AR)
        - Fixed Assets (FA)
        - Cash Management (CM)
        - i-Expense
        - Tax
    - Procure to Pay
        - Purchasing (PO)
- Troubleshoot and diagnose functional incidents
- Perform Oracle patch impact analysis
- Support month-end close, transaction runs and reporting
- Work with the business on day-day data fixes and consolidation process
- Perform root cause analysis (RCA) for critical and repetitive functional tickets
- Coordinate TF incidents with Company technical administration team and 3rd party vendors, including Oracle
- Communicate TF support status to the Client's leadership team
- Act as the Client liaison with software vendors for incident troubleshooting
- Participate in the functional design and testing of customizations to Oracle EBS, as defined by Client
- Functional Change Request (CR) management
    - Initiate, seek approval and execute functional change requests as per approval procedures.
    - Includes:
        - Configuration changes
        - Functional setups
        - Manage, review, execute urgent CR s
        - Follow change management procedures and document changes
- Company assumes that the information provided during TF discussions and through documents is accurate and up-to-date. Result of incorrect information can result in a risk to business systems stability and data integrity and could result in support hours being consumed for rework
- Workaround(s) to production bugs will be suggested by OneNeck team only if they are supported by Oracle
- For any TF or development issues raised by Client, Company shall work each such issue for up to four (4) hours, upon reaching the four-hour limit for any one issue, Company shall contact Client to receive approval to continue the proposed troubleshooting
- Oracle CSR resolution is dependent on the solutions or fixes from Oracle Corporation
- Company assumes that the Client's business users will be available for any discussion required for problem troubleshooting and resolution and will be provided in a timely manner

TF support is provided by USA resident resources and non-USA resident resources (onshore, offshore)

* TF support is limited to the number of hours per month as contracted for this ItemID. Unused hours can roll over and accumulate a max total of 56 hours. The client can use the 56 accumulated hours + 24 hours for a total of 80 hours in a given month (This assumes they have accumulated 56 hours). At the end date of the contract, any unused hours are forfeited. Any hours worked over the accumulated and monthly hours will be billed out at the hourly rate contracted under ItemID 601452.

TF Support Prioritization and Engagement Objectives

- Company will provide support to the Client s Oracle EBS users for TF support through question and issue submission through incident tickets submitted to and administered by Company s help desk, prioritized as follows:

a

Priority	Definition	Support Hours	Engagement Objective during Support Hours
1	One or more business-critical application functions is impeding the customer s ability to perform business.	Monday-Friday, 8am-5pm CDT	30 minutes
2	One or more business-critical application functions are degraded and is impacting the customer s ability to perform business.	Monday-Friday, 8am-5pm CDT	2 hours
3	The incident has a medium impact on the customer's ability to perform business.	Monday-Friday, 8am-5pm CDT	4 hours
4	The incident has a minor impact on the customer's ability to perform business.	Monday-Friday, 8am-5pm CDT	24 hours
5	The incident has no impact on the customer s ability to perform business.	Monday-Friday, 8am-8pm CDT	48 hours

- TF support will be provided on a best-effort basis for any time outside of the designated support hours unless agreed upon in advance by both parties

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Screening Functional Issues
  - Client shall internally review each functional issue and determine the necessity of escalating such issue to Company. This is done to limit unnecessary use of allocated functional support hours
- Oracle EBS Development
  - Code Development
  - Report Development
  - Code troubleshooting and maintenance
- Necessary software licensing to enable functional support staff to access Client systems

601452

Company's Responsibilities and Included Features

Oracle EBS Techno-Functional Support - Onshore-Offshore - Overage Hours is a mandatory add-on component to ItemID 601451 Oracle EBS Financial, Procurement and Project Techno-Functional Support - Onshore-Offshore

Any hours consumed over the hours per month contracted under Item ID 601451 will be billed at the contracted rate for this ItemID 601452.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

601453

Company's Responsibilities and Included Features

Techno-Functional Support*

- Provide Techno-Functional (TF) support in the use of Oracle EBS to Client key end-users in each of the following areas:
  - Financials
    - General Ledger (GL)

        - Accounts Payable (AP)
            - Accounts Receivables (AR)
            - Fixed Assets (FA)
            - Cash Management (CM)
            - Tax
        - Customer Relationship Management (CRM)
            - Telesales
            - Service
        - Procure to Pay
            - Purchasing (PO)
            - Inventory
- Troubleshoot and diagnose functional incidents
- Perform Oracle patch impact analysis
- Support month-end close, transaction runs and reporting
- Work with the business on day-day data fixes and consolidation process
- Perform root cause analysis (RCA) for critical and repetitive functional tickets
- Coordinate TF incidents with Company technical administration team and 3rd party vendors, including Oracle
- Communicate TF support status to the Client's leadership team
- Act as the Client liaison with software vendors for incident troubleshooting
- Participate in the functional design and testing of customizations to Oracle EBS, as defined by Client
- Functional Change Request (CR) management
    - Initiate, seek approval and execute functional change requests as per approval procedures.
    - Includes:
        - Configuration changes
        - Functional setups
        - Manage, review, execute urgent CR s
        - Follow change management procedures and document changes
- Company assumes that the information provided during TF discussions and through documents is accurate and up-to-date. Result of incorrect information can result in a risk to business systems stability and data integrity and could result in support hours being consumed for rework
- Workaround(s) to production bugs will be suggested by OneNeck team only if they are supported by Oracle
- For any TF or development issues raised by Client, Company shall work each such issue for up to four (4) hours, upon reaching the four-hour limit for any one issue, Company shall contact Client to receive approval to continue the proposed troubleshooting
- Oracle CSR resolution is dependent on the solutions or fixes from Oracle Corporation
- Oracle EBS Development
    - Code Development
    - Report Development
    - Code troubleshooting and maintenance
- Company assumes that the Client's business users will be available for any discussion required for problem troubleshooting and resolution and will be provided in a timely manner

TF support is provided by USA resident resources and non-USA resident resources (onshore, offshore)

* TF support is limited to the number of hours per month as contracted for this ItemID. Unused hours will not roll over to subsequent months.

TF Support Prioritization and Engagement Objectives

- Company will provide support to the Client s Oracle EBS users for TF support through question and issue submission through incident tickets submitted to and administered by Company s help desk, prioritized as follows:

a

Priority	Definition	Support Hours	Engagement Objective during Support Hours

1	One or more business-critical application functions is impeding the customer s ability to perform business.	Monday-Friday, 8am-5pm EDT	30 minutes
2	One or more business-critical application functions are degraded and is impacting the customer s ability to perform business.	Monday-Friday, 8am-5pm EDT	2 hours
3	The incident has a medium impact on the customer's ability to perform business.	Monday-Friday, 8am-5pm EDT	4 hours
4	The incident has a minor impact on the customer's ability to perform business.	Monday-Friday, 8am-5pm EDT	24 hours
5	The incident has no impact on the customer s ability to perform business.	Monday-Friday, 8am-8pm EDT	48 hours

- TF support will be provided on a best-effort basis for any time outside of the designated support hours unless agreed upon in advance by both parties

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Screening Functional Issues
  - Client shall internally review each functional issue and determine the necessity of escalating such issue to Company. This is done to limit unnecessary use of allocated functional support hours
- Necessary software licensing to enable functional support staff to access Client systems
- A current Oracle EBS software support agreement with the software provider or alternate 3rd party provider must be in place

611387 Oracle and SplashBI Applications Administration

Company's Responsibilities and Included Features

Company will provide applications administration as described herein. These services will be limited to providing administration of 2 instances of Oracle EBS and 2 instances of SplashBI applications

General Application Administration

- Create users
- Disable users
- Reset password
- Add/remove/extend roles/responsibilities for users
- Update email address
- Update manager
- Update name change of name
- Printer setup/troubleshooting
- Update/modify/add profile options for users/programs/applications
- Schedule/modify/run concurrent program
- Modify default printers for users in EBS
- Workflow Management

Splash BI user management

- SplashBI reports
  - Add new users
  - Reset Passwords

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Category: Other Enterprise Applications

301572 Informatica Data Archive Job Run - Annually

Company's Responsibilities and Included Features

Annual Archive Job Management

- Company to initiate and coordinate the final approval and scheduling of annual archive jobs based upon the predefined archive job schedule.
    - Customer to approve launch of archive jobs.
- Run and monitor archive jobs as currently configured and scheduled
    - All jobs are to be manually scheduled and launched.
    - No automatic job starting will occur.
    - Provide notification of job completion.
- Provide a trigger to the database administration team for large or annual archive jobs to initiate post archive database tuning such as rebuilding indexes.
- Management of job errors. This will be dealt with as follows:
    - Oracle database technical errors (out of space, connectivity, etc.) Escalated to Oracle DBA support to rectify error condition and restart job.
    - Data Error - Escalate to customer to fix data or Company will contact Informatica for vendor provided patch/fix and restart job once rectified.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Errors due to table changes. Major EBS patches could result in schema changes. A time and material project will be required to update the archive job configurations and to rerun the job once rectified.
- Un-archiving of data can be done on a time and material basis.
- The creation of new Oracle EBS archive jobs.
    - Any such work is to be executed as an archiving time and material project.
- Configuration changes, Business rule amendment to existing archive jobs.
    - Code development fixes or enhancements to existing archive jobs.
    - All existing archiving jobs are considered to be fully tested and operationally sound for their intended archiving purpose.
    - These types of changes will be handled in the context of a time and material project effort.
- Any archiving directly within the database or outside of the Informatica ILM defined jobs.
- Recovery of storage space through rebuilding or reorganizing the database.
- Informatica Data Archive for Oracle EBS application administration

301573 Informatica Data Archive Job Run - Monthly

Company's Responsibilities and Included Features

Monthly Archive Job Management

- Company to initiate and coordinate the final approval and scheduling of monthly archive jobs based upon the predefined archive job schedule.
    - Customer to approve launch of archive jobs.
- Run and monitor archive jobs as currently configured and scheduled
    - All jobs are to be manually scheduled and launched.
    - No automatic job starting will occur.
    - Provide notification of job completion.
- Provide a trigger to the database administration team for large or annual archive jobs to initiate post archive database tuning such as rebuilding indexes.

- Management of job errors. This will be dealt with as follows:
  - Oracle database technical errors (out of space, connectivity, etc.) Escalated to Oracle DBA support to rectify error condition and restart job.
  - Data Error - Escalate to customer to fix data or Company will contact Informatica for vendor provided patch/fix and restart job once rectified.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Errors due to table changes. Major EBS patches could result in schema changes. A time and material project will be required to update the archive job configurations and to rerun the job once rectified.
- Un-archiving of data can be done on a time and material basis.
- The creation of new Oracle EBS archive jobs.
  - Any such work is to be executed as an archiving time and material project.
- Configuration changes, Business rule amendment to existing archive jobs.
  - Code development fixes or enhancements to existing archive jobs.
  - All existing archiving jobs are considered to be fully tested and operationally sound for their intended archiving purpose.
  - These types of changes will be handled in the context of a time and material project effort.
- Any archiving directly within the database or outside of the Informatica ILM defined jobs.
- Recovery of storage space through rebuilding or reorganizing the database.
- Informatica Data Archive for Oracle EBS application administration

301574 Informatica Data Archive Job Run - Quarterly

Company's Responsibilities and Included Features

Quarterly Archive Job Management

- Company to initiate and coordinate the final approval and scheduling of quarterly archive jobs based upon the predefined archive job schedule.
  - Customer to approve launch of archive jobs.
- Run and monitor archive jobs as currently configured and scheduled
  - All jobs are to be manually scheduled and launched.
  - No automatic job starting will occur.
  - Provide notification of job completion.
- Provide a trigger to the database administration team for large or annual archive jobs to initiate post archive database tuning such as rebuilding indexes.
- Management of job errors. This will be dealt with as follows:
  - Oracle database technical errors (out of space, connectivity, etc.) Escalated to Oracle DBA support to rectify error condition and restart job.
  - Data Error - Escalate to customer to fix data or Company will contact Informatica for vendor provided patch/fix and restart job once rectified.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Errors due to table changes. Major EBS patches could result in schema changes. A time and material project will be required to update the archive job configurations and to rerun the job once rectified.
- Un-archiving of data can be done on a time and material basis.
- The creation of new Oracle EBS archive jobs.
  - Any such work is to be executed as an archiving time and material project.
- Configuration changes, Business rule amendment to existing archive jobs.
  - Code development fixes or enhancements to existing archive jobs.
  - All existing archiving jobs are considered to be fully tested and operationally sound for their intended archiving purpose.
  - These types of changes will be handled in the context of a time and material project effort.

- Any archiving directly within the database or outside of the Informatica ILM defined jobs.
- Recovery of storage space through rebuilding or reorganizing the database.
- Informatica Data Archive for Oracle EBS application administration

600129 EDI disaster recovery application administration

Company's Responsibilities and Included Features

General

- Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center.
- This service is specific to the administration of a Company managed EDI environment in a Recovery Site acting as a failover environment.
- Replication of the application binaries and file systems from the primary servers to the target DR servers is to be provided through the use of server to server replication software and requires an OS replication Service Item which will perform the replication.
- Company shall develop and maintain Disaster Recovery Failover Procedures.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR EDI environment is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Application Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client
- The number of failover tests per year is referenced in Pricing Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the data was when testing began.

Application Failover Services

- On declaration of a disaster, Company will perform the steps necessary to restart and validate the application on the target DR server and make it the primary application environment, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the primary environment, administration of the Dynamics AX application will be as per the administrative, support, backup and monitoring services as defined for the primary environment.
- Server Failback Services will be provided on a project, time and material basis

Application Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the

Client, schedule and return service back to the Primary Site.

- The application administrator will assist the operating systems administrator reestablish application file system replication back to the target DR server.
- Application Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Third Party Application Dependency Management

- Management of third party application interface to the application
- Administration of third party applications associated with this DR environment.

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

Replication Management

- Configuration of replication policies
- Monitoring of replication services

Diagnosis of replication incidents

- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

600132 Informatica Data Archive disaster recovery application administration

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of an Informatica Data Archiving environment in a Recovery Site, acting as a failover environment.
Replication of the application binaries and file systems from the primary servers to the target DR servers is to be provided through the use of server to server replication software and requires an OS replication Service Item which will perform the replication.
Company shall develop and maintain Disaster Recovery Failover Procedures.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Application Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client
- The number of failover tests per year is referenced in Pricing Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the data was when testing began.

Application Failover Services

On declaration of a disaster, Company will perform the steps necessary to restart and validate the application on the target DR server and make it the primary application environment, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
During the period that the target DR server is acting as the primary environment, administration of the Oracle Demantra application will be as per the administrative, support, backup and monitoring services as defined for the primary environment.

Application Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The application administrator will assist the operating systems administrator reestablish application file system replication back to the target DR server.
- Application Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Third Party Application Dependency Management

- Management of third party application interface to the application
- Administration of third party applications associated with this DR environment.

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

600140 Third party application disaster recovery administration

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of an application environment in a Recovery Site acting as a failover environment.

Replication of the application binaries and file systems from the primary servers to the target DR servers is to be provided through the use of server to server replication software, storage replication, or hypervisor replication and requires an OS replication Service Item which will perform the replication.
Company shall develop and maintain Disaster Recovery Failover Procedures.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Application Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client
- The number of failover tests per year is referenced in Pricing Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the data was when testing began.

Application Failover Services

On declaration of a disaster, Company will perform the steps necessary to restart and validate the application on the target DR server and make it the primary application environment, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
During the period that the target DR server is acting as the primary environment, administration of the Oracle Agile application will be as per the administrative, support, backup and monitoring services as defined for the primary environment.

Application Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The application administrator will assist the operating systems administrator reestablish application file system replication back to the target DR server.
- Application Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Third Party Application Dependency Management

- Management of third party application interface to the application
- Administration of third party applications associated with this DR environment.

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

600162 Baan application administration

Company's Responsibilities and Included Features

Application Administration

Manage the following areas within the Baan Applications suite:

- User provisioning and security within Baan
- Services Monitoring
- Cloning environments
- Clone application and refresh database from production to non-production environment.
- Quantity of clones provided is referenced in the Service Parameters

Device Maintenance.

- Printer Configuration. Manage the printer configurations for the relevant operating systems and Baan software.
- Device Queue Maintenance. Manage the Baan Device Queue for stopped queues as well as the periodic purging of Device Queues.

Batch Jobs.

- Batch Job Maintenance. Provide maintenance for existing non-interactive applications (Batch Jobs).
- Monitor the delivery of the Batch Jobs, their execution time, and the amount of server resources required by such Batch Jobs and will update any minor changes.
- Batch Job Creation. Create and place into production Batch Jobs based on Client requirements. It will be Client s responsibility to determine and document its requirements and submit the change via the Systems Change Request. Create and test the Batch Job in Baan as appropriate.

Custom object change management

- Migration of customizations through Development, Test, QA environments (as applicable) through to production
- Change control

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Engagement of software providers Help Desk support (requires Client to have a support contract with the software provider)
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues
- Provide client with updates

Document user issues and system errors

Patching and Upgrades

Standard Patch Maintenance - Company shall provide patch application where patches for Baan are within the following criteria:

- One-off patches - Patch to address a specific failure to standard functionality (i.e. Break-Fix)
- Any single or group of Baan patches (Service Pack) required to solve a single or multiple failures to standard functionality
- Hot-fix roll-ups or kernel only updates
- The patching activity is not associated with an Baan version upgrade
- The patching activity is not associated with a database version upgrade

Custom Code Management - Company shall provide patch application for customized Baan code/objects where patches are within the following criteria:

- One-off patches - Patch to address a specific failure to customized functionality (i.e. Break-Fix)
- Any single or group of customized Baan code/object patches required to solve a single or multiple failures to customized functionality
- The patching activity is not associated with an Baan version upgrade
- The patching activity is not associated with a database version upgrade

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

3rd Party Application Support

Any 3rd party application running on the Baan servers or interfacing to Baan are not included in the scope of this Service Item but may be supported under additional Service Items.

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

End user Support and Management

- Support of non-super users
- Application functional support
- Application Development

600165 EDI Application and Transaction Administration

Company's Responsibilities and Included Features

EDI Application Administration

- Services Monitoring
- Create and issue EDI user ID s and passwords only if Client uses client software
- Maintain a test/development environment as required for EDI
- Upon clients request Company will kill user processes in the operating system
- Document issues and or application errors
- Maintain rigorous change control of all system changes
- Engagement of software providers Help Desk Support

EDI Transaction Administration

- Monitor delinquent functional acknowledgement report and research and resolve any discrepancies received
- Check all email received from EDI translator throughout the day for errors in translation or communication
- Execute monthly archiving of inbound and outbound data (i.e X12 and/or EDIFACT)
- All requests/projects will be required to have a ticket opened for monitoring purposes
- Advise Client EDI Manager of issues
- Update ticket as appropriate based on solution or failures or projects
- Mapping changes will require Client approval

Resend EDI documents as appropriate Acknowledge any tickets opened by Company Monitoring tools Ensure successful translation of inbound/outbound EDI documents per Trading Partner requirements Validate all data

inbound/outbound has been received/sent successfully via VAN, AS2 or FTP communications Assist client in diagnosing and analyzing functional issues as they pertain to EDI

Patching and Upgrades
Standard Patch Maintenance as required Company shall apply patches when necessary for EDI software for the following criteria:

- One-off patches Patch to address a specific failure to standard functionality (i.e. Break-fix)
- Patch testing will only occur if a test system has been provided
- Testing will only include one document for each transaction type

Major Upgrades Any Major release upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the parties.

- Upgrades will be performed as needed to maintain software support
- Test system will be required
- All documents for each Client/supplier will be tested

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Engagement of software providers Help Desk support (requires Client to have a support contract with the software provider)
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues
- Provide client with updates

Document user issues and system errors

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Software Licensing

- Procurement of application software and licensing for current version of EDI software, for a minimum of two users
- Providing software for editing data (i.e. UltraEdit)
- Procurement of current software support and maintenance
- Procurement of communication software when EDI software does not meet EDI communications requirements
- Company is not responsible for client software installation and support

Application Database Administration

- Administration of databases as required by the application

ERP Application Development and Support

- ERP application functional support related EDI transaction processing and error rectification in ERP application
- ERP application customization or configuration in support of EDI
- ERP data corrections
- ERP cross-reference data

600299 Baan disaster recovery application administration

Company's Responsibilities and Included Features

General

- Company shall provide disaster recovery services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of a Baan environment in a Recovery Site acting as a failover environment.
- Replication of the application binaries and file systems from the primary servers to the target DR servers is to be provided through the use of server to server replication software and requires an OS replication Service Item which will perform the replication.
- Company shall develop and maintain disaster recovery failover procedures.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Application Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client
- The number of failover tests per year is referenced in Service Parameters
- During failover testing the disaster recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster occur during a test the data will be as old as the data was when testing began.

Application Failover Services

- On declaration of a disaster, Company will perform the steps necessary to restart and validate the application on the target DR server and make it the primary application environment, operational and accessible on the DR network as defined in the disaster recovery failover procedures.
- During the period that the target DR server is acting as the primary environment, administration of the Baan application will be as per the administrative, support, backup and monitoring services as defined for the primary environment.

Application Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the disaster recovery failover procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The application administrator will assist the operating systems administrator reestablish application file system replication back to the target DR server.
- Application failback services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Third Party Application Dependency Management

- Management of third party application interface to the application
- Administration of third party applications associated with this DR environment.

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

600561 Baan Functional Support

Company's Responsibilities and Included Features

Baan Functional Support

- Provide functional support to key and end users in the use of Baan V ERP environment with the Client s current architecture of the Finance-Logistic configuration and the number of Baan companies up to 1350 named end users
- Provide triage and troubleshooting for functional incidents including batch jobs failures
- Work with application admin for troubleshooting issues with interface applications as documented below
- Act as the Client liaison with software vendors of Baan and third-party applications and interfaces listed below for incident troubleshooting
- Functional Change Request (CR) management
- Initiate, seek approval and execute functional change requests as per approval procedures.
- All initiatives or business drivers to update, improve or enhance the functionality or the Baan environment or to implement new modules or functionality over and above 40 hours of functional resources per initiative will require a separate SOW so as not to impede on the day to day support of the Baan environment.
- Full Time Equivalent (FTE) is defined as a resource or a combination of resources available for up to 40 hours per week, 52 weeks a year to perform work
- Support will be provided with the following resourcing types and levels:
  - 2 FTE Baan logistics and finance - for functional support
  - 0.25 FTE Baan development - for software debugging
  - 0.25 FTE Project management - for Baan tickets support, Baan ticket coordination

Baan Functional support responsibility incudes these third-party applications and interfaces as defined:

- Tradebeam: management of interface files along or sales order blocking
- SFI (Shop Floor Information): for user issues were Baan data configurations are causing reporting errors
- OCC: collaborate with the Client s BizTalk team to perform manual corrections in Baan
- Global Sales Forecasting: collaborate with Baan administrator for batch job execution
- LIMS Labware: collaborate with the Client s LIMS administrator on issues /questions related to interface processing
- Web Reporting: collaborate with Client s Web reporting team to address inaccurate data reporting
- Maximo: assign incident to the Client s application owners for support
- FRx: technical support as a third-party application
- WERCS: collaborate with Client s Baan development team on any processing related issues
- Wireless Warehouse: assign incident to the Client s application owners for support
- Loftware: assign incident to the Client s application owners for support
- QITS (Quality Issues Tracking): assign incident to the Client s application owners for support
- Cognos: assign incident to the Client s application owners for support
- Wonderware: assign incident to the Client s application owners for support
- OpenWorld: assign incident to the Clients s application owners for support
- BizTalk: assign incident to the Client s application owners for support

Support Prioritization

Support requests will be prioritized as follows:

First Level - To support the Client s Baan ERP users with questions and issue resolution as defined through trouble tickets administered by Company s Support Center

Second Level - To participate in the functional design and testing of customizations to Baan ERP, as defined by Client

Third Level - To participate in any additional projects or initiatives required by Client

Functional support is provided during the business hours of 6:00 AM EST to 6:00 PM PST, Monday through Friday, excluding normal Client holidays.

Support outside the above business hours will be provided for priority 1 and 2 issues.

Priority is assessed based on impact and urgency of incident.

Priority and Service Level Targets

Priority	Timescale	Response Target
1	24x7x365	15 minutes
2	24x7x365	2 hours
3	M-F, 6:00 AM EST to 6:00 PM PST	12 business hours
4	M-F, 6:00 AM EST to 6:00 PM PST	24 business hours
5	M-F, 6:00 AM EST to 6:00 PM PST	24 business hours

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Screening Functional Issues

- Provide access to Client s ticketing system for functional support resources
- Users will call Client s helpdesk for all urgent (P1 and P2) issues
- Client s helpdesk to call Company s helpdesk for all P1 & P2 incidents
- Baan Development
- Baan Administration

601252 Baan Development

Company's Responsibilities and Included Features

Baan Development Support:

- Provide development support for Baan IV environment to develop new or modify existing customizations
- Assist Baan functional support personnel with debugging of application data issues
- Assist Baan technical personnel with application patch or related research
- Develop technical specification based upon functional requirements provided
- Conduct unit and integration testing with assistance from functional support personnel
- Document Baan development using customization administration methods

Baan Development is limited to the number of hours per month as contracted. Unconsumed support hours will not be rolled over to the next month.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Baan Development Environment

- Provide Baan development environment infrastructure
- Provide Company only access to Baan development environment
- Infor support agreement
- Provide necessary user licensing for Company developers<p style="font-family: Calibri; font-size: 10pt; font-weight: bold;">

601504

Company's Responsibilities and Included Features

Functional Support*

- Provide functional support in the use of Infor LN software to Client key end users in each of the following areas:
  - Procure to Pay
    - RFQs
    - Purchasing (PO)
    - Vendor management
  - Sales order processing
    - Sales order entry
    - Commission/rebates
    - Pricing
  - Inventory Management and Warehousing
    - Inbound receipt process
    - Outbound shipping process
    - Inventory enquiries
  - Manufacturing and Quality
    - Shop floor control
    - Non Conforming Material Report (NCMR) Process
    - Material issues and backflushing
  - Product Management and Engineering

        - Item setup and attributes
        - Bill of Materials (BOM) issues
        - Routing
- Troubleshoot and diagnose functional incidents
- Work with business key contacts on day-day data fixes and consolidation process
- Perform root cause analysis (RCA) for critical and repetitive functional tickets
- Coordinate incidents with Company technical administration team and 3rd party vendors, including Infor
- Communicate support status to the Client's leadership team
- Act as the Client liaison with software vendors for incident troubleshooting
- Participate in the functional design and testing of customizations to Infor LN, as defined by Client
- Functional change request (CR) management
    - Initiate, seek approval and execute functional change requests as per approval procedures.
    - Includes:
        - Configuration changes
        - Functional setups
        - Manage, review, execute urgent CR s
        - Follow change management procedures and document changes
- Company assumes that the information provided during functional discussions and through documents is accurate and up-to-date.
- Company is not responsible for result of incorrect information, which can result in a risk to business systems stability and data integrity and could result in support hours being consumed for rework
- Workaround(s) to production bugs will be suggested by OneNeck team only if they are supported by Infor
- For any functional issues raised by Client, Company shall work each such issue for up to four (4) hours, upon reaching the four-hour limit for any one issue, Company shall contact Client to receive approval to continue the proposed troubleshooting
- Infor CSR resolution is dependent on the solutions or fixes from Infor

Functional support is provided by non-USA resident resources (offshore)

* Functional support is limited to the number of hours per month as contracted, based upon a rolling three (3) month average of hours consumed. Bursts in monthly consumption may not exceed 10% of contracted monthly hours.

Functional Support Prioritization and Engagement Objectives

- Company will provide support to the Client s Infor LN users for functional support through question and issue submission through incident tickets submitted to and administered by Client s help desk

Priority	Definition	Support Hours	Initial Engagement Target during Support Hours
1	One or more business-critical application functions is impeding the customer s ability to perform business.	Monday-Friday, 6am-6pm CT	30 minutes
2	One or more business-critical application functions are degraded and is impacting the customer s ability to perform business.	Monday-Friday, 6am-6pm CT	2 hours
3	The incident has a medium impact on the customer's ability to perform business.	Monday-Friday, 6am-6pm CT	4 hours
4	The incident has a minor impact on the customer's ability to perform business.	Monday-Friday, 6am-6pm CT	24 hours
	The incident has no impact on the customer s ability to perform	Monday-	

5	business.	Friday, 6am-6pm CT	48 hours

- Functional support will be provided on resource availability for any requests outside of the designated support hours unless agreed upon in advance by both parties

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Screening Functional Issues
  - Client shall internally review each functional issue and determine the necessity of escalating such issue to Company. This is done to limit unnecessary use of allocated functional support hours
- Infor LN Development
  - Code Development
  - Report Development
  - Code troubleshooting and maintenance
- Necessary software licensing for Infor and as required to enable Company functional support staff to access Client systems
- Company assumes that the Client's business users will be available for any discussion required for problem troubleshooting and resolution and will be provided in a timely manner

Family: Hardware and Software

Category: Arrow Financial Services

601237 ARROW Waukee, IA Sales tax

Company's Responsibilities and Included Features

Baan Functional Support

- Provide functional support to key and end users in the use of Baan V ERP environment with the Client s current architecture of the Finance-Logistic configuration and the number of Baan companies up to 1350 named end users
- Provide triage and troubleshooting for functional incidents including batch jobs failures
- Work with application admin for troubleshooting issues with interface applications as documented below
- Act as the Client liaison with software vendors of Baan and third-party applications and interfaces listed below for incident troubleshooting
- Functional Change Request (CR) management
- Initiate, seek approval and execute functional change requests as per approval procedures.
- All initiatives or business drivers to update, improve or enhance the functionality or the Baan environment or to implement new modules or functionality over and above 40 hours of functional resources per initiative will require a separate SOW so as not to impede on the day to day support of the Baan environment.
- Full Time Equivalent (FTE) is defined as a resource or a combination of resources available for up to 40 hours per week, 52 weeks a year to perform work
- Support will be provided with the following resourcing types and levels:
  - 2 FTE Baan logistics and finance - for functional support
  - 0.25 FTE Baan development - for software debugging
  - 0.25 FTE Project management - for Baan tickets support, Baan ticket coordination

Baan Functional support responsibility incudes these third-party applications and interfaces as defined:

- Tradebeam: management of interface files along or sales order blocking
- SFI (Shop Floor Information): for user issues were Baan data configurations are causing reporting errors
- OCC: collaborate with the Client s BizTalk team to perform manual corrections in Baan
- Global Sales Forecasting: collaborate with Baan administrator for batch job execution
- LIMS Labware: collaborate with the Client s LIMS administrator on issues /questions related to interface processing

- Web Reporting: collaborate with Client s Web reporting team to address inaccurate data reporting
- Maximo: assign incident to the Client s application owners for support
- FRx: technical support as a third-party application
- WERCS: collaborate with Client s Baan development team on any processing related issues
- Wireless Warehouse: assign incident to the Client s application owners for support
- Loftware: assign incident to the Client s application owners for support
- QITS (Quality Issues Tracking): assign incident to the Client s application owners for support
- Cognos: assign incident to the Client s application owners for support
- Wonderware: assign incident to the Client s application owners for support
- OpenWorld: assign incident to the Clients s application owners for support
- BizTalk: assign incident to the Client s application owners for support

Support Prioritization

Support requests will be prioritized as follows:

First Level - To support the Client s Baan ERP users with questions and issue resolution as defined through trouble tickets administered by Company s Support Center

Second Level - To participate in the functional design and testing of customizations to Baan ERP, as defined by Client

Third Level - To participate in any additional projects or initiatives required by Client

Functional support is provided during the business hours of 6:00 AM EST to 6:00 PM PST, Monday through Friday, excluding normal Client holidays.

Support outside the above business hours will be provided for priority 1 and 2 issues.

Priority is assessed based on impact and urgency of incident.

Priority and Service Level Targets

Priority	Timescale	Response Target
1	24x7x365	15 minutes
2	24x7x365	2 hours
3	M-F, 6:00 AM EST to 6:00 PM PST	12 business hours
4	M-F, 6:00 AM EST to 6:00 PM PST	24 business hours
5	M-F, 6:00 AM EST to 6:00 PM PST	24 business hours

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Screening Functional Issues

- Provide access to Client s ticketing system for functional support resources
- Users will call Client s helpdesk for all urgent (P1 and P2) issues
- Client s helpdesk to call Company s helpdesk for all P1 & P2 incidents
- Baan Development
- Baan Administration

Category: Hardware

601263 Cisco ISR 4451 AX Bundle with APP and SEC license

Company's Responsibilities and Included Features

Provide a Cisco ISR 4451 Router AX Bundle with APP and SEC license on a monthly subscription basis.

Bill of Materials

Ln#	Qty	Part #	Description
1	1	ISR4451-X-AX/K9	Cisco ISR 4451 AX Bundle with APP and SEC license
2	1	CON-SNTP-ISR4X51-X	3 YR SNTC-24X7X4 Cisco ISR 4451 AppX
3	1	SL-44-IPB-K9	IP Base License for Cisco ISR 4400 Series
4	1	MEM-4400-4GU16G	4G to 16G DRAM Upgrade (8G+8G) for Cisco ISR 4400
5	1	MEM-FLASH-8U32G	8G to 32G Compact Flash Memory Upgrade for Cisco ISR 4450
6	1	PWR-4450-AC	AC Power Supply for Cisco ISR 4450 and ISR4350
7	1	PWR-4450-AC/2	AC Power Supply (Secondary PS) for Cisco ISR 4450
8	2	CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m
9	1	MEM-4400-DP-2G	2G DRAM (1 DIMM) for Cisco ISR 4400 Data Plane
10	1	WAAS-RTU-2500	WAAS and VWAAS Right to Use for 2500 connections
11	1	CON-ECMU-WS2500	3 YR SWSS UPGRADES WAAS and VWAAS Right
12	2	POE-COVER-4450	Cover for empty POE slot on Cisco ISR 4450
13	1	ISRWAAS-RTU-2500	ISRWAAS RTU for 2500 connections
14	1	SL-44-APP-K9	AppX License for Cisco ISR 4400 Series
15	1	NIM-BLANK	Blank faceplate for NIM slot on Cisco ISR 4400
16	1	SL-44-SEC-K9	Security License for Cisco ISR 4400 Series
17	2	SM-S-BLANK	Removable faceplate for SM slot on Cisco 2900,3900,4400 ISR
18	1	SISR4400UK9-169	Cisco ISR 4400 Series IOS XE Universal

Repair and SLO

- The Service Level Objective (SLO) for repair or replacement is next business day or better.

Service Renewal

- This service's availability for renewal is at the Company's discretion.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Contract for Managed Services on the device.
- Equipment must be colocated (housed) within one of the Company s data centers.
- Return the equipment to Company upon the end of Term.

601471

Company's Responsibilities and Included Features

Provide an HPE DL360 G10 - 4 x Core - 64GB - FC HBA on a monthly subscription basis.

Bill of Materials

Ln#	Qty	Part #	Description
1	1	867959-B21	HPE DL360 Gen10 8SFF CTO Server
2	1	867959-B21 ABA	U.S. - English localization
3	1	860659-L21	HPE DL360 Gen10 Xeon-S 4112 FIO Kit
4	4	815098-B21	HPE 16GB 1Rx4 PC4-2666V-R Smart Kit
5	4	815098-B21 0D1	HPE 16GB 1Rx4 PC4-2666V-R Smart Kit Factory integrated
6	1	P9D94A	HPE SN1100Q 16Gb 2p FC HBA
7	1	P9D94A 0D1	HPE SN1100Q 16Gb 2p FC HBA Factory integrated
8	2	865408-B21	HPE 500W FS Plat Ht Plg LH Pwr Sply Kit
9	2	865408-B21 0D1	Factory integrated
10	2	R1C65A	HPE C13-C14 IN 250V 2m Blk Jumper Cord
11	2	R1C65A 0D1	Factory integrated
12	1	BD505A	HPE iLO Adv 1-svr Lic 3yr Support
13	1	BD505A 0D1	Factory integrated
14	1	741279-B21	HPE Dual 8GB microSD EM USB Kit
15	1	741279-B21 0D1	HP Dual 8GB microSD EM USB Kit Factory integrated
16	1	874543-B21	HPE 1U Gen10 SFF Easy Install Rail Kit
17	1	874543-B21 0D1	Factory integrated
18	1	H1K92A3	HPE 3Y Proactive Care 24x7 Service
19	1	H1K92A3 R2M	iLO Advanced Non Blade - 3yr SW Supp
20	1	H1K92A3 WAG	HPE 3Y Proactive Care 24x7 Service

Repair and SLO

- The Service Level Objective (SLO) for repair or replacement is next business day or better.

Service Renewal

- This service's availability for renewal is at the Company's discretion.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Contract for Managed Services on the device.
- Equipment must be colocated (housed) within one of the Company s data centers.
- Return the equipment to Company upon the end of Term.

601472

Company's Responsibilities and Included Features

Provide an HPE DL360 G10 - 6 x Core - 128GB - FC HBA on a monthly subscription basis.

Bill of Materials

Ln#	Qty	Part #	Description
1	1	867959-B21	HPE DL360 Gen10 8SFF CTO Server
2	1	867959-B21 ABA	U.S. - English localization
3	1	860685-L21	HPE DL360 Gen10 Xeon-G 6128 FIO Kit
4	4	815100-B21	HPE 32GB 2Rx4 PC4-2666V-R Smart Kit
5	4	815100-B21 0D1	HPE 32GB 2Rx4 PC4-2666V-R Smart Kit Factory integrated
6	1	P9D94A	HPE SN1100Q 16Gb 2p FC HBA
7	1	P9D94A 0D1	HPE SN1100Q 16Gb 2p FC HBA Factory integrated
8	2	865408-B21	HPE 500W FS Plat Ht Plg LH Pwr Sply Kit
9	2	865408-B21 0D1	Factory integrated
10	2	R1C65A	HPE C13-C14 IN 250V 2m Blk Jumper Cord
11	2	R1C65A 0D1	Factory integrated
12	1	BD505A	HPE iLO Adv 1-svr Lic 3yr Support
13	1	BD505A 0D1	Factory integrated
14	1	741279-B21	HPE Dual 8GB microSD EM USB Kit
15	1	741279-B21 0D1	HP Dual 8GB microSD EM USB Kit Factory integrated
16	1	874543-B21	HPE 1U Gen10 SFF Easy Install Rail Kit
17	1	874543-B21 0D1	Factory integrated
18	1	H1K92A3	HPE 3Y Proactive Care 24x7 Service
19	1	H1K92A3 R2M	iLO Advanced Non Blade - 3yr SW Supp
20	1	H1K92A3 WAG	HPE 3Y Proactive Care 24x7 Service

Repair and SLO

- The Service Level Objective (SLO) for repair or replacement is next business day or better.

Service Renewal

- This service's availability for renewal is at the Company's discretion.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Contract for Managed Services on the device.
- Equipment must be colocated (housed) within one of the Company s data centers.
- Return the equipment to Company upon the end of Term.

601520

Company's Responsibilities and Included Features

Provide a CiscoCSR 1000V router, AX Bundle with e-PAK 3-year subscription .

Bill of Materials

Ln#	Qty	Part #	Description
1	1	L-CSR-50M-AX-3Y=	CSR 1000V e-PAK 3-year subscription 50Mbps AX Package
2	1	CON-ECMU-LCSR5MAY	3 Year - SWSS UPGRADES CSR 1000V e-PAK 1-year subscription 50Mbps AX

Repair and SLO

- The Service Level Objective (SLO) for repair or replacement is next business day or better.

Service Renewal

- This service's availability for renewal is at the Company's discretion.
- Company will provide Client with at least 60 days notification ahead of contract end of term of this ItemId of the Company s intent not to renew the availability of this ItemId or within 30 days of OEM notifying Company of end of sale or end of life of the ItemId whichever occurs later.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Contract for Managed Services on the device.
- Equipment must be colocated (housed) within one of the Company s data centers.
- Return the equipment to Company upon the end of Term.

601522

Company's Responsibilities and Included Features

Provide a Catalyst 9200L 24-port data, 4 x 1G, with Network Essentials switch

Bill of Materials

Ln#	Qty	Part #	Description
1	1	C9200L-24T-4G-E	Catalyst 9200L 24-port data, 4 x 1G, Network Essentials
2	1	CON-SNTP-C920L24T	SNTC-24X7X4 Catalyst 9200L 24-port data, 4 x 1G, Net
3	1	C9200L-NW-E-24	C9200L Network Essentials, 24-port license
4	1	CAB-TA-NA	North America AC Type A Power Cable
5	1	PWR-C5-BLANK	Config 5 Power Supply Blank
6	1	C9200L-DNA-E-24	C9200L Cisco DNA Essentials, 24-port Term license
7	1	C9200L-DNA-E-24-3Y	C9200L Cisco DNA Essentials, 24-port, 3 Year Term license
8	1	C9200L-STACK-KIT	Cisco Catalyst 9200L Stack Module
9	2	C9200-STACK	Catalyst 9200 Stack Module
10	1	STACK-T4-50CM	50CM Type 4 Stacking Cable
11	1	NETWORK-PNP-LIC	Network Plug-n-Play Connect for zero-touch device deployment

Repair and SLO

- The Service Level Objective (SLO) for repair or replacement is next business day or better.

Service Renewal

- This service's availability for renewal is at the Company's discretion.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Contract for Managed Services on the device.
- Equipment must be colocated (housed) within one of the Company s data centers.
- Return the equipment to Company upon the end of Term.

601798 1000BASE-T SFP transceiver modules and U.S. Export Restriction Compliance license for 4400 series

Company's Responsibilities and Included Features

Provide 1000BASE-T SFP transceiver module for Category 5 copper wire interfaces and U.S. Export Restriction Compliance license for 4400 series

Bill of Materials

Ln#	Qty	Part #	Description
1	28	GLC-TE=	1000BASE-T SFP transceiver module for Category 5 copper wire
2	3	FL-44-HSEC-K9=	U.S. Export Restriction Compliance license for 4400 series

Repair and SLO

- The Service Level Objective (SLO) for repair or replacement is next business day or better.

Service Renewal

- This service's availability for renewal is at the Company's discretion.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Contract for Managed Services on the device.
- Software and hardware must be colocated (housed) within one of the Company s data centers.
- Return the equipment to Company upon the end of Term.

Category: Software

600342 Red Hat Enterprise Linux Server for Service Providers, Full Support (Physical or Virtual Nodes) (Dedicated) (Monthly)

Company's Responsibilities and Included Features

Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Red Hat offerings will be made and provided by Red Hat, Inc., and may be subject to change as determined by Red Hat, Inc. Company may revise terms of use or pricing at any time to reflect Red Hat s updates to its terms or pricing. Client agrees that the Red Hat Offerings are subject to Red Hat s Subscription Services Agreement available at https://www.redhat.com/licenses/cloud_cssa/GLOBAL_Cloud_Software_Subscription_Agreement_English_20171117.pdf , which are hereby incorporated into this Statement of Work.

Provide support subscription from Red Hat for Red Hat Enterprise Linux, Client dedicated, physical or virtual nodes which

provides Company administrators access to Red Hat for the following services:

- Installation
- Usage
- Configuration
- Diagnosis
- Bug reports (dependent on product life cycle)
- Bug fixes
- Red Hat Extras channel

No direct access from Client to Red Hat is provided.

May not be used on an Oracle VM Platform

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

600652 Red Hat Enterprise Linux Server for Virtual Datacenters, Full Support (Physical or Virtual Nodes) (Dedicated) (Monthly)

Company's Responsibilities and Included Features

Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Red Hat offerings will be made and provided by Red Hat, Inc., and may be subject to change as determined by Red Hat, Inc. Company may revise terms of use or pricing at any time to reflect Red Hat s updates to its terms or pricing. Client agrees that the Red Hat offerings are subject to Red Hat s Subscription Services Agreement available at https://www.redhat.com/licenses/cloud_cssa/GLOBAL_Cloud_Software_Subscription_Agreement_English_20171117.pdf , which are hereby incorporated into this Statement of Work.

Provide support subscription from Red Hat for Red Hat Enterprise Linux Server for Virtual Datacenters, Full Support (dedicated physical or virtual nodes) which provides Company administrators access to Red Hat for the following services:

- Installation
- Usage
- Configuration
- Diagnosis
- Bug reports (dependent on product life cycle)
- Bug fixes
- Red Hat Extras channel

No direct access from Client to Red Hat is provided.

May not be used on an Oracle VM Platform

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

601489

Company's Responsibilities and Included Features

Provide a VMware vSphere v.6.0 Enterprise Plus - 1 Processor - Upgrade License on a monthly subscription basis.

Client can purchase the license after the end of the 24-month term at the fair market price.

Bill of Materials

Ln#	Qty	Part #	Description
1	1	none	VMware vSphere v.6.0 Enterprise Plus - Upgrade License - 1 Processor

Repair and SLO

- The Service Level Objective (SLO) for repair or replacement is next business day or better.

Service Renewal

- This service's availability for renewal is at the Company's discretion.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

601493

Company's Responsibilities and Included Features

Provide a 1 year Cisco Intersight license on a monthly subscription basis.

Bill of Materials

Ln#	Qty	Part #	Description
1	incl	DC-MGT-SAAS	Cisco Intersight SaaS
2	1	DC-MGT-SAAS-EST-C	Cisco Intersight SaaS - Essentials
3	1	DC-MGT-IMCS-1S	IMC Supervisor - Advanced - 1 Server License
4	1	DC-MGT-UCSC-1S	UCS Central Per Server - 1 Server License
5	1	SVS-DCM-SUPT-BAS	Basic Support for DCM

Service Renewal

- This service's availability for renewal is at the Company's discretion.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

601494

Company's Responsibilities and Included Features

Provide a 1 Year VMWare Support and Subscription on a monthly subscription basis.

Bill of Materials

Ln#	Qty	Part #	Description
1	1	-	VMware Support and Subscription Production - 1 Year - Service - 24 x 7 x 30 Minute - Technical - Electronic Service

Service Renewal

- This service's availability for renewal is at the Company's discretion.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

601521

Company's Responsibilities and Included Features

Provide a license for Cisco Unified Border Element (CUBE) SIP Session

Bill of Materials

Ln#	Qty	Part #	Description
1	1	L-CUBE	Cisco Unified Border Element (CUBE) - E-delivery - top level
2	1	CON-ECMU-LCUBE001	3 Year - SWSS UPGRADES Cisco Unified Border Element (CUBE) - E-
3	1	CUBE-T-RED	CUBE - 1 Redundant Trunk Session License
4	1	CON-ECMU-CUBETRDE	3 Year - SWSS UPGRADES CUBE Redundant Trunk Single Session - 1

Repair and SLO

- The Service Level Objective (SLO) for repair or replacement is next business day or better.

Service Renewal

- This service's availability for renewal is at the Company's discretion.
- Company will provide Client with at least 60 days notification ahead of contract end of term of this ItemId of the Company s intent not to renew the availability of this ItemId or within 30 days of OEM notifying Company of end of sale or end of life of the ItemId whichever occurs later.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Contract for Managed Services on the device.
- for use on equipment colocated (housed) within one of the Company s data centers.
- Return the licensing to Company upon the end of Term

601796 Cisco Firepower Management Center,(VMWare) for 10 devices

Company's Responsibilities and Included Features

Provide a Cisco Firepower Management Center for VMWare for 10 devices on a monthly subscription basis.

Bill of Materials

Ln#	Qty	Part #	Description
1	1	FS-VMW-10-SW-K9	Cisco Firepower Management Center,(VMWare) for 10 devices

2 1 CON-ECMUS-VMWSW10 SOLN SUPP SWSS Cisco Firepower Management Center,(VMWare)

Repair and SLO

- The Service Level Objective (SLO) for repair or replacement is next business day or better.

Service Renewal

- This service's availability for renewal is at the Company's discretion.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Contract for Managed Services on the device.
- Equipment must be colocated (housed) within one of the Company s data centers.
- Return the equipment to Company upon the end of Term.

611333 Red Hat Enterprise Linux Server, Full Support (1 to 8 vCPUs per Virtual Node, Multi-Tenant, Monthly)

Company's Responsibilities and Included Features

Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Red Hat offerings will be made and provided by Red Hat, Inc., and may be subject to change as determined by Red Hat, Inc. Company may revise terms of use or pricing at any time to reflect Red Hat s updates to its terms or pricing. Client agrees that the Red Hat offerings are subject to Red Hat s Subscription Services Agreement available at https://www.redhat.com/licenses/cloud_cssa/GLOBAL_Cloud_Software_Subscription_Agreement_English_20171117.pdf , which are hereby incorporated into this Statement of Work.

Provide support subscription from Red Hat Enterprise Linux Server, Full Support (1 to 8 vCPUs per Virtual Node, Multi-Tenant, Monthly) which provides Company administrators access to Red Hat for the following services:

- Installation
- Usage
- Configuration
- Diagnosis
- Bug reports (dependent on product life cycle)
- Bug fixes
- Red Hat Extras channel

No direct access from Client to Red Hat is provided.

May not be used on an Oracle VM Platform

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

None

611334 Red Hat Enterprise Linux Server, Full Support (9 to 127 vCPUs per Virtual Node, Multi-Tenant, Monthly)

Company's Responsibilities and Included Features

Client agrees, acknowledges, and understands that the actual manufacture, provision, and performance of the Red Hat offerings will be made and provided by Red Hat, Inc., and may be subject to change as determined by Red Hat, Inc. Company may revise terms of use or pricing at any time to reflect Red Hat s updates to its terms or pricing. Client agrees that the Red Hat

offerings are subject to Red Hat s Subscription Services Agreement available at https://www.redhat.com/licenses/cloud_cssa/GLOBAL_Cloud_Software_Subscription_Agreement_English_20171117.pdf , which are hereby incorporated into this Statement of Work.

Provide support subscription from Red Hat Enterprise Linux Server, Full Support (9 to 127 vCPUs per Virtual Node, Multi-Tenant, Monthly) which provides Company administrators access to Red Hat for the following services:

- Installation
- Usage
- Configuration
- Diagnosis
- Bug reports (dependent on product life cycle)
- Bug fixes
- Red Hat Extras channel

No direct access from Client to Red Hat is provided.

May not be used on an Oracle VM Platform

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

None

Family: Managed Services

Category: Backup

611724 Commvault Cloud Clean Room Recovery SaaS Administration

Commvault Cloud Cleanroom Recovery ("Cleanroom") provides a clean, secure, isolated recovery environment on demand for testing cyber recovery plans and conducting secure forensic analysis.

Company will provide setup and removal of validation environment using a secure cloud environment on a quarterly basis. The service requires use of Commvault Cloud Air Gap Protect storage. .

Definitions

- Cleanroom Recovery Validation – Test recovery of recovery group or entities for validation.

Service Parameters

- Validations are limited to four (4) quarterly recoveries per year.
- Recovery period is limited to four (4) days between clean room recovery and removal of all resources
- Effort – Effort is limited to eight (8) hours per Cleanroom Recovery Validation
- Test Virtual Machine ("VM") Limit – limit of up to twenty (20) VMs per Cleanroom Recovery Validation Test size – Based of off licensing capacity
- Test size – Based of off licensing capacity

Company's Responsibilities and Included Features

Cleanroom Recovery

- Perform recovery planning session
- Prepare empty Azure environment
- Restore Control Plane using the CommServe Recovery Service
- Restore Active Directory/Azure Active Directory

- Restore a recovery group or entity into a Cleanroom site
- Provide access for validation

Cleanroom Removal

- Recovery closure
- Documentation updates
- Remove all resources

Terms

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month-to-month basis.
- Company may revise the terms of use or pricing with 30 days' notice.

Service Delivery

- Designated Company key point of contact
- Recoveries for validation are to be scheduled in advance

Expert User Technical Support*

- Technical support may only be requested by a Client Expert User*, available during the following hours
  - 7 am to 7 pm MST, Monday to Friday technical support for priority 1, 2, 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client Validation

- Provide quarterly validation windows
- Provide subject matter experts for validation of environment
- Perform validation of systems and applications
- Declare closure of validation period

Production Environment

- No changes to be made to production as part of this service.

Initial Cleanroom Implementation and Resource Configuration

- Cleanroom implementation is not included in this administrative service and is a pre-requisite for service execution.
- Onboarding and configuration of recovery groups, entities and targets is part of the setup of individual resources and not included in this service.

On-demand Cleanroom Recoveries

- On-demand Cleanroom recoveries are available as separate project.

Disaster Recovery and Disaster Recovery Environment

- Cleanroom is meant for periodic testing and validation of systems to scan for malware. Actual cyber recovery, forensic analysis, and business recovery in the event of a security breach is available as separate project.

Remediation of Malware

- Remediation of malware is not included in this service

Azure Subscriptions

- Client must provide the Azure subscription(s) to be used for Cleanroom Recovery
- Verify that the Cleanroom recovery site is an Azure subscription and tenant that has never been accessed by production accounts and is isolated from the production site.
- Provide Azure resources consumed during Cleanroom Recovery Validations

Design, Deploy, Migration and Administration

- Perform setup, configuration, migration and administration of Azure Resources, integrations, data and applications, including but not limited to:
  - VM
  - Azure Active Directory
  - Active Directory
  - Azure AD connect integration
  - Network integrations and settings outside of Azure
- Runbook activities to maintain resources and applications
- Perform backup & restore operations
- Azure resource monitoring
- Azure alert monitoring
- Remediation of Azure environment from audit findings or assessments
- Project work

Commvault Cloud Backup Licensing

- Procure software and licensing for Commvault Cloud
- Use of Commvault Cloud Air Gap Protect storage

Category: Disaster Recovery

601423 Azure Site Recovery Replication Management

Company's Responsibilities and Included Features

Overview

Client has selected Azure Site Recovery (ASR) to provide Disaster Recovery (DR) services to provide service continuity in the event of a failure that prevents the delivery of services from the primary data center. Client requires Company to monitor and manage these services on behalf of Client.

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of Microsoft support

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backward from the point of disaster.
- The replication policies for this service will be configured to achieve an agreed-upon RPO; however, this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service will be defined after the first DR test

Server Failover Testing

- Server failover testing will be limited to one test per year
- DR testing is limited to failover to a network isolated from production and during the DR test the production environment/s continue to operate.
- DR failover testing will be conducted in collaboration with the Client.
- DR failover testing must be scheduled at least 1 calendar month in advance.
- Company is limited to bringing up the servers only and performing either a ping test or ARM console validation under boot diagnostics.
- Maintenance of server failover testing runbook.

Server Failover Services

- On the declaration of a disaster, Company will perform the steps necessary to activate the target DR server and make it the active server, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- Company is limited to bringing up the servers only and performing either a ping test or ARM console validation under boot diagnostics.
- During the period that the target DR server is acting as the active server, administration of the server will be as per the administrative, support, backup and monitoring services as defined for the primary server.
- Maintenance of server failover runbook.

Server Failback Services

- When the ability to provide services from the primary server is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the primary site.
- Reestablishment of replication back to the target DR server will then be activated and services will return to normal operational mode
- Server Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Expert-to-expert helpdesk support:

- 24 x 7 technical support for priority 1 and 2 incidents
- 8/5 technical support for priority 3, 4 and 5 incidents

* An Expert User is defined as a Client designated person with an in-depth application or system knowledge who is a designated Client contact for initiating or escalating incidents to Company limited to 5 total defined experts or 5% of the Client's staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Azure Resources

An Azure subscription with the following services:

- Azure Site Recovery
- Storage Services

- ExpressRoute or VPN services

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

DR Workload Configuration and Testing

Configuration, testing, and management of the operating system, databases, and applications during:

- Failover testing
- DR failover
- DR failback

Client Side DR Configuration and Testing

- Configurations of end-user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.
- Client-side network changes

Microsoft Azure Subscription

- Azure subscription and resources needed to support Azure Site Recovery
- Provide Azure monitoring resources, Azure Monitor and Log Analytics for service monitoring
- Provide Company access to Azure Subscriptions and Resource Groups
- Provide Company access to the Azure VM and OS

601444 Zerto Disaster Recovery Software as a Service with Management - Dedicated

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery (DR) software as a service for the purpose of providing the virtual server replication service as part of a full DR plan. This service is specific to providing and maintaining the software used to manage and provide replication of virtual servers from the primary data center to the disaster recovery data center and to provide the technical administration and tools to administer DR tests and/or conduct a DR failover in the case of a DR event is declared.

- Requires: 600272 - DRaaS - Virtual Replication Service licensing (per VM) setup

Disaster Recovery Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Disaster Recovery Replication Software Patch Management

- Replication software patch management of both the primary and target DR locations and servers
- Up to quarterly routine review same-version patch analysis and application
- Application of updates and patches during approved maintenance windows
- Up to one application version upgrade every two years

Replication Management

- Configuration of replication policies
- Maintain DR test and failover configuration
- Maintain DR test and failover procedures for the servers up to and including the operating system and Company s data center network reconfiguration during DR testing or failover

Monitoring of replication services
- Triage and troubleshooting of replication incidents
- Engagement of replication software providers help desk support

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- RPO will be limited by the network bandwidth available for replication of data from the primary servers to the target DR data center and the rate of change on the primary servers. RPO will be monitored and managed for variance outside the reasonably acceptable norms for the Client s specific environments.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- An RTO will be set after deployment of the DR environment and initial failover test have been conducted

Server Failover Testing

- One (1) annual failover test for this service will be conducted in collaboration with the Client.
- The duration of the annual DR test will be limited to 48 hours
- Failover testing is limited to collaboration and troubleshooting with the Client until the OS boots up
- DR testing will be conducted in an isolated DR test network without stopping source environments

Server Failover Services

- On declaration of a disaster, Company will perform the steps necessary to activate the target DR servers and make them the active servers, operational and accessible on the DR network as defined in DR failover procedures.
- Failover is limited to collaboration and troubleshooting with the Client until the OS boots up
- During the period that the target DR server is acting as the active server, administration of the server will be as per the administrative, support, backup and monitoring services as defined for the primary server

Server Failback Services

- When the ability to provide services from the primary server is restored, Company will initiate failback to the primary server as documented in the DR failover procedures, and in collaboration with the Client, schedule and return service back to the primary site.
- Reestablishment of replication back to the target DR server will then be activated and services will return back to normal operational mode
- Server Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

End User Terms and Conditions

Client certifies and agrees that use of the software is subject to the Zerto Professional Services - End User Terms and Conditions (EULA), which may be amended by Zerto from time to time at their discretion. A current copy of the EULA is posted at https://www.zerto.com/wp-content/uploads/2017/09/Zerto-Professional-Services-End-User-Terms-and-Conditions.pdf. Client may be required to accept a click-wrap version of the EULA prior to access and use of the Zerto software.

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

DR Configuration

Inform Company of changes to:

- DR recovery retention window
- Server startup sequencing and startup delay
- Network mapping
- Server re-IP plan (if applicable)

Virtualization Platform

- Virtualization platform with sufficient capacity in the source (production) and target (DR) datacenters
- Capacity must include the necessary capacity for the DR replication software servers/virtual appliances
- Virtualization platform host hardware (Disk, CPU and RAM)
- Virtualization software on which the virtual machine being managed is run
- Management of virtualization platform

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

Local Area Network (LAN) and Wide Area Network (WAN)

- Management of LAN
- Management of WAN
- Execution of all LAN or WAN changes necessary for DR Failover or DT Failover testing

Applications and Client-Side DR Configuration and Testing

- Maintain DR test and failover procedures for all databases and applications existing on the servers included in the DR plan
- Database and application management and reconfiguration during DR testing or failover
- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Conducting functional and data validation testing during server failover testing.

602531 Nutanix Leap Disaster Recovery Policy Administration

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery (DR) administration of Nutanix Leap for the purpose of providing the virtual server replication and recovery service as part of a DR plan. This service solely applies to:

- Maintaining the configuration of the recovery policies used to define replication of Virtual Machine (VM)
- Maintaining the Leap recovery plan for recovery from the primary data center to the disaster recovery data center
- Providing the technical administration of DR tests and/or
- Conducting a DR failover in the case a DR event is declared.

Requires: 602540 - Nutanix Leap Disaster Recovery (per VM) setup

Replication and Recovery Plan Management

- Configuration of replication policies
- Maintain DR test and failover recovery plans for the virtual servers and Company s data center network reconfiguration for DR testing or DR failover
- Monitoring of replication services
- Triage and troubleshooting of replication incidents
- Engagement of replication software providers help desk support

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backward from the point of disaster.
- RPO will be limited by the network bandwidth available for replication of data from the primary servers to the target DR data center and the rate of change on the primary servers. RPO will be monitored and managed for variance outside the reasonably acceptable norms for the Client s specific environments.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- An RTO will be set after deployment of the DR environment and an initial failover test has been conducted

Server Failover Testing

- One (1) annual failover test for this service will be conducted in collaboration with the Client.
- Annual failover testing must be at least scheduled 6 weeks in advance
- The duration of the annual DR test will be limited to 48 hours, with a Company s level of effort limited to 3 hours of engineer/administrator time per VM
- DR testing will be conducted in an isolated DR test network without stopping source environments
- DR testing by Company is limited to ensuring that the VM boots up in the sequence defined in the recovery/test plan

Server Failover Services

- On declaration of a disaster, Company will undertake to activate the target DR servers and make them the active servers, operational and accessible on the DR network as defined in DR failover procedures.
- Rerouting network traffic
- During the period that the target DR server is acting as the active server, administration of the server will be as per the administrative, support, backup and monitoring services as defined for the primary server

Server Failback Services

- When the ability to provide services from the primary server is restored, Company will initiate failback to the primary server as documented in the DR failover procedures, and in collaboration with the Client, schedule and return service back to the primary site.
- Reestablishment of replication back to the target DR server will then be activated and services will return back to normal operational mode
- Server Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the

OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Disaster Recovery Replication Software Licensing - (Typically included in ReliaCloud Edge products)

- Procurement of Nutanix Leap DR orchestration software and licensing for the current version of Leap
- Procurement of current software maintenance where applicable

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions, and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Disaster Recovery

- Declaration of a disaster to initiate a recovery plan. The need to declare a disaster should be discussed with Company before declaring the disaster to ensure that this is the best course of action.
- Executing any/all recovery plan actions needed within the operating system, database or applications
- Coordination with WAN circuit providers to re-route WAN traffic during a DR event

DR Configuration

Inform Company of changes to:

- DR recovery retention window
- Server startup sequencing and startup delay
- Network mapping
- Server re-IP plan (if applicable)

Virtualization Platform

- Virtualization platform with sufficient capacity in the source (production) and target (DR) datacenters
- Capacity must include the necessary capacity for the DR replication software servers/virtual appliances
- Virtualization platform host hardware (Disk, CPU and RAM)
- Virtualization software on which the virtual machine being managed is run
- Management of virtualization platform
- Provide Company with access to the Client's production cluster to enable administration of Nutanix DR

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

Operating System, Database network and Applications and Client-Side DR Configuration and Testing

- Maintain DR test and failover procedures for all operating systems, databases, and applications existing on the servers included in the DR plan
- Operating system, database and application management, and reconfiguration during DR testing or failover
- Configurations of end-user devices and/or Client infrastructure that are required to allow end-users to access the environment.
- Conducting functional and data validation testing during server failover testing.

602540 Nutanix Leap Disaster Recovery (per VM) setup

Company's Responsibilities and Included Features

- Initial setup and configuration of Nutanix Leap Recovery Policy for the Virtual Machine (VM) or adding the VM to an existing Nutanix Leap Recovery Policy. Includes:
  - Setup of replication
  - Setup of recovery plan
- Guide Customer with the installation of Nutanix guest tools on VM where necessary

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Requires: 602531 - Nutanix Leap Disaster Recovery Policy Administration
- Define Customer process for initiation and approval of a declaration of a disaster which initiates the DR fail-over of the VM
- DR testing and/or testing simulation of deployed recovery policy and associated recovery plan
- Install Nutanix guest tools on VM where necessary
- Configure Disaster Recovery (DR) networks in Nutanix clusters and cluster's spine-leaf networks

Category: Managed Applications

103038-N Managed Citrix XenServer Server Setup

Company's Responsibilities and Included Features

- Receive, unpack and install device in rack
- Cabling (power, KVM, network, HBA, SAN)
- Firmware updates
- Rapid deployment setup
- OS installation, configuration and OS updates / patches
- 3rd party tool installation (backup, anti-virus, monitoring)
- Documentation updates (portal, tasks, support center)
- Configure and verify backups and monitoring

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

103039 Application Monitoring Only (per Application)

Company's Responsibilities and Included Features

- Deploy and configure monitoring of application using Company standard template
- Supported technologies:
  - All applications supported under Company managed services
- Configure monitoring of:
  - Application specific services

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Resolve issues identified by Company monitoring
- Provide appropriate escalation path for alerts
- Work with Company to adjust and tune alerting thresholds
- Provide appropriate credentials to enable monitoring
- Configure network and devices to meet monitoring requirements

500076 Dedicated Citrix Foundation Application Management (100 user minimum)

Company's Responsibilities and Included Features

Citrix services availability management Licensing Server

- Manage service availability for Citrix license service
- Report license usage
- Apply license packages as required Storefront Server
- Storefront portal availability management
- Monitor and manage IIS worker process for Storefront
- Monitor and manage Storefront services
- Maintain stores communication paths to dependent systems
- Manage store configuration profiles Director Server
- Monitor and manage IIS worker process for Director
- Maintain Director communication paths to dependent system
- Review historical trends for performance tuning, issue management, and capacity planning Delivery Controller
- Application and desktop publishing and deployment management (excludes image and application packaging)
- Session based delivery management
- Manage global and individual Citrix policies
- User rights administration
- Monitor and manage Citrix broker services
- Maintain Delivery Controller communication path
- Manage user assignments
- Citrix policy implementation and management as directed by the Client
- Citrix Security Configuration Standard reporting:
    - Monthly License usage report
    - Monthly System usage report
- Citrix infrastructure log maintenance and reviews
- Advanced system administration support for Citrix infrastructure issues

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Requires Company infrastructure managed services (Hypervisor and/or OS management)
- Supported version 7.x or greater
- End use device management
- Network connectivity
- Printer device management
- End user support
- Client must provide required public SSL certificate(s)
- Server hardware support or management
- Desktop image and management
- Application package and management
- Application dependencies
- Procurement of Citrix application software and licensing, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable
- Support in the following areas of the applications loaded onto Citrix:
    - Functional support
    - Configuration, management or support of the application from within the packaged application
- Application issue triage and resolution

- Application patch identification

500077 Dedicated Citrix Foundation Application Management (201-500 users)

Company's Responsibilities and Included Features

Citrix services availability management Licensing Server

- Manage service availability for Citrix license service
- Report license usage
- Apply license packages as required Storefront Server
- Storefront portal availability management
- Monitor and manage IIS worker process for Storefront
- Monitor and manage Storefront services
- Maintain stores communication paths to dependent systems
- Manage store configuration profiles Director Server
- Monitor and manage IIS worker process for Director
- Maintain Director communication paths to dependent system
- Review historical trends for performance tuning, issue management, and capacity planning Delivery Controller
- Application and desktop publishing and deployment management (excludes image and application packaging)
- Session based delivery management
- Manage global and individual Citrix policies
- User rights administration
- Monitor and manage Citrix broker services
- Maintain Delivery Controller communication path
- Manage user assignments
- Citrix policy implementation and management as directed by the Client
- Citrix Security Configuration Standard reporting:
    - Monthly License usage report
    - Monthly System usage report
- Citrix infrastructure log maintenance and reviews
- Advanced system administration support for Citrix infrastructure issues

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Requires Company infrastructure managed services (Hypervisor and/or OS management)
- Supported version 7.x or greater
- End use device management
- Network connectivity
- Printer device management
- End user support
- Client must provide required public SSL certificate(s)
- Server hardware support or management
- Desktop image and management
- Application package and management
- Application dependencies
- Procurement of Citrix application software and licensing, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

- Support in the following areas of the applications loaded onto Citrix:
  - Functional support
  - Configuration, management or support of the application from within the packaged application
- Application issue triage and resolution
- Application patch identification

500078 Dedicated Citrix Foundation Application Management (501-1000 users)

Company's Responsibilities and Included Features

Citrix services availability management Licensing Server

- Manage service availability for Citrix license service
- Report license usage
- Apply license packages as required Storefront Server
- Storefront portal availability management
- Monitor and manage IIS worker process for Storefront
- Monitor and manage Storefront services
- Maintain stores communication paths to dependent systems
- Manage store configuration profiles Director Server
- Monitor and manage IIS worker process for Director
- Maintain Director communication paths to dependent system
- Review historical trends for performance tuning, issue management, and capacity planning Delivery Controller
- Application and desktop publishing and deployment management (excludes image and application packaging)
- Session based delivery management
- Manage global and individual Citrix policies
- User rights administration
- Monitor and manage Citrix broker services
- Maintain Delivery Controller communication path
- Manage user assignments
- Citrix policy implementation and management as directed by the Client
- Citrix Security Configuration Standard reporting:
  - Monthly License usage report
  - Monthly System usage report
- Citrix infrastructure log maintenance and reviews
- Advanced system administration support for Citrix infrastructure issues

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Requires Company infrastructure managed services (Hypervisor and/or OS management)
- Supported version 7.x or greater
- End use device management
- Network connectivity
- Printer device management
- End user support
- Client must provide required public SSL certificate(s)
- Server hardware support or management
- Desktop image and management
- Application package and management

- Application dependencies
- Procurement of Citrix application software and licensing, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable
- Support in the following areas of the applications loaded onto Citrix:
    - Functional support
    - Configuration, management or support of the application from within the packaged application
- Application issue triage and resolution
- Application patch identification

500079 Dedicated Citrix Foundation Application Management (1000+ users)

Company's Responsibilities and Included Features

Citrix services availability management Licensing Server

- Manage service availability for Citrix license service
- Report license usage
- Apply license packages as required Storefront Server
- Storefront portal availability management
- Monitor and manage IIS worker process for Storefront
- Monitor and manage Storefront services
- Maintain stores communication paths to dependent systems
- Manage store configuration profiles Director Server
- Monitor and manage IIS worker process for Director
- Maintain Director communication paths to dependent system
- Review historical trends for performance tuning, issue management, and capacity planning Delivery Controller
- Application and desktop publishing and deployment management (excludes image and application packaging)
- Session based delivery management
- Manage global and individual Citrix policies
- User rights administration
- Monitor and manage Citrix broker services
- Maintain Delivery Controller communication path
- Manage user assignments
- Citrix policy implementation and management as directed by the Client
- Citrix Security Configuration Standard reporting:
    - Monthly License usage report
    - Monthly System usage report
- Citrix infrastructure log maintenance and reviews
- Advanced system administration support for Citrix infrastructure issues

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Requires Company infrastructure managed services (Hypervisor and/or OS management)
- Supported version 7.x or greater
- End use device management
- Network connectivity
- Printer device management
- End user support

- Client must provide required public SSL certificate(s)
- Server hardware support or management
- Desktop image and management
- Application package and management
- Application dependencies
- Procurement of Citrix application software and licensing, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable
- Support in the following areas of the applications loaded onto Citrix:
    - Functional support
    - Configuration, management or support of the application from within the packaged application
- Application issue triage and resolution
- Application patch identification

500081 Dedicated Citrix MCS Management (per user - 100 user miniumum)

Company's Responsibilities and Included Features

- Management of template VM
    - Creation and management of Machine Catalogs
    - Creation and management of Delivery Groups
    - Storage allocation requirements (Collaboration with Storage resource)
    - Network connectivity requirements (Collaboration with Network resource)
- Monitor and maintain API Connections to the hypervisor and Active Directory
- Manage schedule image release to production users (Limit of 2 releases per image per month)
    - Manage end user maintenance notifications
    - Conduct end user system log off and image reboot process
    - Monitor and verify image copy process
- Advanced system administration support for MCS issues
    - Troubleshoot image Push failures o Revert to previous image

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Supported versions 7.x or greater
- Storage device configuration and management
- Network device configuration and management
- Hypervisor configuration and management
- Active Directory configuration and management

500082 Dedicated Citrix PVS Management (100-200 users - 100 user minimum)

Company's Responsibilities and Included Features

- Manage and maintain PVS services
    - Site creation
    - vDisk Stores
    - Version control (up to 5 previous versions)
    - Device Collection Groups
    - Boot Device Management configuration
- Management of template VM
    - Creation and management of Machine Catalogs
    - Creation and management of Delivery Groups

        - Storage allocation requirements (Collaboration with Storage resource)
        - Network connectivity requirements (Collaboration with Network resource)
    - Monitor and maintain API Connections to the hypervisor, PVS database, and Active Directory
    - Manage schedule image promotion to production users (Limit of 4 promotions per image per month)
        - Manage end user maintenance notifications
        - Conduct end user system log off and image reboot process
        - Monitor and verify image promotion process
    - Advanced system administration support for PVS issues
        - Troubleshoot image Promotion failures o Revert to previous image

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Supported versions 7.x or greater
- Storage device configuration and management
- Network device configuration and management
- Hypervisor configuration and management
- Active Directory configuration and management

500083 Dedicated Citrix PVS Management (201-500 users)

Company's Responsibilities and Included Features

- Manage and maintain PVS services
    - Site creation
    - vDisk Stores
    - Version control (up to 5 previous versions)
    - Device Collection Groups
    - Boot Device Management configuration
- Management of template VM
    - Creation and management of Machine Catalogs
    - Creation and management of Delivery Groups
    - Storage allocation requirements (Collaboration with Storage resource)
    - Network connectivity requirements (Collaboration with Network resource)
- Monitor and maintain API Connections to the hypervisor, PVS database, and Active Directory
- Manage schedule image promotion to production users (Limit of 4 promotions per image per month)
    - Manage end user maintenance notifications
    - Conduct end user system log off and image reboot process
    - Monitor and verify image promotion process
- Advanced system administration support for PVS issues
    - Troubleshoot image Promotion failures
    - Revert to previous image

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Supported versions 7.x or greater
- Storage device configuration and management
- Network device configuration and management
- Hypervisor configuration and management
- Active Directory configuration and management

500084 Dedicated Citrix PVS Management (501-1000 users)

Company's Responsibilities and Included Features

- Manage and maintain PVS services
    - Site creation
    - vDisk Stores
    - Version control (up to 5 previous versions)
    - Device Collection Groups
    - Boot Device Management configuration
- Management of template VM
    - Creation and management of Machine Catalogs
    - Creation and management of Delivery Groups
    - Storage allocation requirements (Collaboration with Storage resource)
    - Network connectivity requirements (Collaboration with Network resource)
- Monitor and maintain API Connections to the hypervisor, PVS database, and Active Directory
- Manage schedule image promotion to production users (Limit of 4 promotions per image per month)
    - Manage end user maintenance notifications
    - Conduct end user system log off and image reboot process
    - Monitor and verify image promotion process
- Advanced system administration support for PVS issues
    - Troubleshoot image Promotion failures
    - Revert to previous image

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Supported versions 7.x or greater
- Storage device configuration and management
- Network device configuration and management
- Hypervisor configuration and management
- Active Directory configuration and management

500085 Dedicated Citrix PVS Management (1000+ users)

Company's Responsibilities and Included Features

- Manage and maintain PVS services
    - Site creation
    - vDisk Stores
    - Version control (up to 5 previous versions)
    - Device Collection Groups
    - Boot Device Management configuration
- Management of template VM
    - Creation and management of Machine Catalogs
    - Creation and management of Delivery Groups
    - Storage allocation requirements (Collaboration with Storage resource)
    - Network connectivity requirements (Collaboration with Network resource)
- Monitor and maintain API Connections to the hypervisor, PVS database, and Active Directory
- Manage schedule image promotion to production users (Limit of 4 promotions per image per month)

Manage end user maintenance notifications
    - Conduct end user system log off and image reboot process
    - Monitor and verify image promotion process
- Advanced system administration support for PVS issues
    - Troubleshoot image Promotion failures
    - Revert to previous image

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Supported versions 7.x or greater
- Storage device configuration and management
- Network device configuration and management
- Hypervisor configuration and management
- Active Directory configuration and management

500086 VDI/DaaS Application Package Creation, Maintenance and Management - Per Request

Company's Responsibilities and Included Features

Custom application is defined as any application that is dedicated and configured for a single client's usage. E.g. the packaged application cannot be reused without modification for another client. Standard applications packages are not subject to this services and are defined in Company's Packaged Application Catalog.

- Consultation with client to ascertain the specific requirements of the application package to be created and/or any updates or modifications to be made
- Conduct evaluation of requested application via AppDNA to determine application packaging feasibility
- Create application package of a currently supported Microsoft or Linux OS based applications and/or drivers based on AppDNA results
- Modification or update of application package upon client request
- Facilitate user acceptance testing of application package
- Maintain up to 2 previous application package versions

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Request application package modification or update
- Application media and licensing
- Completion of application intake form
- Facilitate client resource assignments and actively assist with UAT process. Not to exceed 10 business days upon UAT release. Support in the following areas of the applications:
    - Functional Support
    - Configuration, management or support of the application from within the packaged application
    - Application issue triage and resolution

500087 VDI/DaaS Image Maintenance and Management Per Image

Company's Responsibilities and Included Features

- Consultation with client to ascertain the specific requirements of the image to be created and/or any updates or modifications to be made
- Installation of a currently supported Microsoft or Linux OS and/or driver updates requested by the client
- Installation of validated drivers specific to the image
- Installation of AppDNA approved applications into the base image whose installation does not require specific

knowledge or expertise

- Modification or update of base image limited to minor version upgrade/updates and patches
- Removal or modification of any installed applications in the base image; excluding any applications that require specific knowledge or expertise
- Facilitate user acceptance testing based on image deployment method
- Maintain up to 5 previous image versions
- Limit of 2 image updates per month

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- OS and application media and licensing
- Completion of application intake form
- Facilitate client resource assignments and actively assist with UAT process. Not to exceed 10 business days upon UAT release. Support in the following areas of the applications:
  - Functional Support
  - Configuration, management or support of the application from within the packaged application
  - Application issue triage and resolution

500088 Citrix XenMobile Mobile Device Management (XDM) management (per user, 100 user minimum)

Company's Responsibilities and Included Features

- XenMobile Device Manager (XDM) application availability management
  - Support limited to current supported versions by Citrix
- NetScaler configuration management for XDM services including:
  - VIP
  - PKI
  - Traffic policies
  - Authentication policies
- NetScaler Connector monitoring and maintenance
- Active Directory integration management
  - Integrate with LDAP to perform user authentication and to manage group policies
- XDM device policy implementation and management as directed by the client
  - Limited to major mobile platforms
  - Mobile policies based on OS and patch levels, passcodes, device ownership, apps and device resources, platform-specific policies, encryption, device status and location
- XDM -> device resets, connection quarantine and troubleshooting
- Mobile device security and compliance management:
  - Security and compliance across device platforms including:
    - Rooting and jailbreak detection
    - Pre-enrollment device checks
    - Geo-fencing and tracking
    - Context-aware policie
    - App blacklist/whitelist
    - Full or selective wipe of devices
- Maintenance for delegation of move, add, change of XDM accounts via Active Directory to client expert contacts
- Deployment and administration of centralized management console for multi-site deployments (As supported by Citrix)
- Support over-the-air provisioning and self-service enrollment

- Support mobile application connectors to the Enterprise App Store Apple device prerequisites (client must register for an Apple distribution account). There are two types:
  - Enterprise (Enterprise accounts are strongly recommended)
  - Developer
- Monthly reporting:
  - Groups
  - Users
  - Roles summary
  - Hardware inventory report
  - Jailbroken or rooted devices
  - Inactive devices
  - Device enrollment
  - Blacklist and whitelist application compliance report
- Advanced system administration support for XenMobile Device Manager infrastructure issues

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Requires infrastructure support (Hypervisor and/or OS mgt)
- Mobile device support
- XenMobile Device Manager licensing
- NetScaler Licensing
- client must provide public SSL certificate for the NetScaler
- Apple device prerequisites
  - Client must register for an Apple distribution account and provide a certificate from the Apple Push Notification service (APNs)
- Multi-factor single sign-on
- Backups of proprietary data, which may be covered under another SKU
- End user support, which may be covered under another SKU

500182 Microsoft Exchange Management - Co-managed

Company's Responsibilities and Included Features

- Administering permissions, rules, policies, and security settings
- Auditing exchange server usage
- Configuring compliance and messaging retention
- Configuring mailbox delivery restrictions, permissions, and storage limits
- Managing databases and storage groups
- Creating and managing database availability groups
- Managing mailbox and public folder databases
- Managing web and mobile access
- SSL certificate management
- Configuring outlook anywhere / RPC over HTTPS
- Configuring POP3 and IMAP4
- Managing Exchange Server features for mobile devices
- Messaging policy and compliance management
- Configuring transport rules
- Configuring and managing journaling

- Configuring and managing archiving
- Optimizing message processing, logging, and anti-spam filtering
- Working with SMTP connectors, sites, and links
- Managing message pickup, replay, throttling, and back pressure
- Creating and managing accepted domains
- Creating and managing e-mail address policies
- Creating and managing remote domains
- Configuring anti-spam and message filtering options
- System maintenance, monitoring, and queuing monitoring
- Troubleshoot issues in the following system areas:
    - Services
    - Resource usage
    - Queues upgrade
    - Periodic review of critical patches
    - Up to quarterly routine review same version patch analysis and application
    - Application of same version updates and patches during approved maintenance windows
    - Any Major release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis
- Availability SLA does not apply to co-managed applications

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Application Software Licensing
- Configuring standard permissions for Exchange server
- Configuring role-based permissions for Exchange server
- Managing user accounts and mail features
- Managing contacts
- Managing distribution list
- Managing offline address books
- Managing online address lists
- Managing mailboxes
- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable
- End user support and management
- Support of end users
- Application functional support
- Content or data related support
- Email client support
- Availability of application, as SLA does not apply to co-managed applications

500183 Microsoft Active Directory Management - Co-managed

Company's Responsibilities and Included Features

- Administration of a single forest, single domain including:
  - Local DNS configurations
  - Implement Active Directory roles (FSMO/GC placement)
  - AD sites and subnets definition
  - Creation of site(s)
  - Creation of AD replication topology
  - Creation of inter-site connectors
  - Creation of subnets and assigned to site(s)
  - Implement OU container structure
  - Implement logon scripts (limited to printer and drive mapping)
  - Implement group policy objects
  - Implement security groups and distribution groups
  - Delegation of administrative roles
  - Domain controller promotions
  - Domain controller demotions
  - Removal of Active Directory roles (FSMO or GC)
  - Removal of domain controller object from sites and subnets
- Availability SLA does not apply to co-managed applications

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Domain user administration
- Provisioning of Active Directory domain users
- Define Active Directory domain policy including:
  - Group membership updates
  - Password resets
  - Account lockout resets
  - User naming standards
  - Account password policy
  - Account Lockout policy
  - User add/change/delete policy
  - Security policies
- Administration of advanced identity or credential managements system, i.e:
  - Biometric identities
  - Smart cards
  - RSA tokens
- Termination of Active Directory domain users
- Password resets
- Availability of application, as SLA does not apply to co-managed applications

600000 Atlas Application Support

Company's Responsibilities and Included Features

Application User Administration

Management of user identities within the application:

- User ID adds, changes, deletes

Security group/role maintenance as applicable to the application as defined by the Client

Incident Triage and Troubleshooting

Company will triage and manage the troubleshooting process for technical system errors.
Company will research problems and issues utilizing:

- Company knowledge of known errors and their solution
- General operating system level troubleshooting
- Escalation to software provider
- Application of Company known solutions
- Application of software vendor provided solutions

Engagement of software providers Help Desk support
Document user issues and system errors

Patching and Upgrades

Standard Patch Maintenance - Company shall provide patch application where patches for the application are within the following criteria:

- One-off patches - Patch to address a specific failure to standard functionality (i.e. Break-Fix)
- Any single or group of patches (Service Pack) required to solve a single issue or required by software vendor
- The patching activity is not associated with an application version upgrade

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

* An Expert User is defined as an application or system knowledge holder and a single point of contact for escalating incidents to Company limited to 5 total defined experts or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

Development Support

Provide application development resources to develop new or modify existing configurations, extensions, modifications, localizations and integrations

- Develop technical specification based upon functional requirements
- Develop or modify application objects
- Develop or modify reports
- Conduct unit and integration testing
- Document customizations

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

600001 Informatica Data Archive for Oracle EBS application administration

Company's Responsibilities and Included Features

Application Administration

Manage the following areas within the Informatica Data Archiving Applications suite:

- Security management
- User access management
- Administrator access management

Application monitoring

- Job monitoring
- Performance monitoring
- Will work with the DBA's to resolve performance issues

Basic Configuration and setup of archive jobs

- Company will provide support for simple changes to the archive job schemas
- Initial setup of all archive jobs to be provide by Client or Oracle EBS functional support provider

Change control

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Engagement of software providers Help Desk support (requires Client to have a support contract with the software provider)
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues
- Provide client with updates

Document user issues and system errors

Patching and Upgrades

Application patching includes research and application of critical updates, recommended patches, updates, and security patches

Break-Fix Patching - Break-Fix patch application will follow the incident priority response SLA

Informatica Data Archiving Break-Fix patching is defined as - A patch or series of patches required by Informatica to rectify an error in the application code of Informatica Data Archiving functionality that has already been implemented, tested and is in production in the Client's environment and include any individual patches, dependent patch sets, required to addressed cuClientpecific Informatica Data Archiving application issues in functionality that has already been implemented, tested and is in production in the custClientvironment, and any Informatica recommended critical patch needed to address known issues

affecting a customClientronment
Non Break-Fix Patching - Non Break-Fix patching requires a 5 business day notification for planning.
The following are types of patches which are not deemed to be Non Break-Fix:

- New functionality
- New architecture
- New modules
- Minor and major version upgrades

Major Version Upgrades - Any major version upgrades, will be treated on a time and material basis and shall be planned and billed to Client as agreed upon by the Parties

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Database Management

- Client to provide management or to have contracted Company to provide database management for the underlying Informatica database, the Oracle EBS database and the Archive database.

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

Application Initial Configuration

- Setup and configuration of all Oracle EBS archive jobs
- Definition of what is to be archived
- Definition of when archiving is to happen
- Definition of who has access to the Archiving application and to the archived data
- Company will do minor ongoing changes to archive jobs due to minor schema changes

600006 Microsoft Management Reporter

Company's Responsibilities and Included Features

System Administration

Manage the following areas within Microsoft Management Reporter:

- Access Control
- Application Patching

24x7x365 Help desk support

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Engagement of software providers Help Desk support (requires Client to have a support contract with the software provider)
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues
- Provide client with updates

Document user issues and system errors

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Report Development

- Development of custom reports
- Support of custom reports

600008 Oracle Application Express (APEX) administration

Company's Responsibilities and Included Features

Application Administration

Manage the following areas within the Oracle Application Express environment:

- Management and monitoring of Oracle Application Express server services including the following components
    - Infrastructure
        - User/Metadata Repository Schema
        - Oracle Application Express listener
        - Oracle Express engine
        - Embeddded PL/SQL gateway
- Workspace provisioning
- Password management of administrative accounts
- Configuration and management of data sources
- System configuration file updates as needed relative to break-fix, security, performance or application requirements
- Routine log file maintenance and purge activity as necessary
- Capacity planning
- Troubleshooting and performance tuning

Incident Diagnosis and Troubleshooting

- Diagnosis of system incidents
- Troubleshooting of system incidents
- Engagement of Oracle support
    - Where necessary Company will engage and log service requests with Oracle to rectify software issues
    - Provide client with updates
- Document user issues and system errors

Patching and Upgrades

Break-Fix Patching - Break-fix patch application will follow the incident priority response SLA

- A Break-Fix patch is defined as a patch or series of patches required by Oracle to rectify an error in the application code

Non Break-Fix Patching* - The following are types of patches which are not deemed to be Break-Fix:

- Minor and major version upgrades
- Quarterly Consolidated Patch Upgrade (CPU)
- Maintenance Release

*Requires a 5 business day notification for planning

Patch application is limited to 12 hours per year. Hours exceeding this will be billed on a time and materials basis with prior written approval by the Client

Patch application includes research and installation of Oracle iAS patches, in all iAS instances, by an Oracle Application Admin

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Functional Support

- Provide functional support in the use of the application to key and end users.
- Diagnosing and resolving functional incidents

Development Support

Provide application development resources to develop new or modify existing configurations, extensions, modifications, localizations and integrations

- Develop technical specification based upon functional requirements
- Develop or modify application objects
- Develop or modify reports
- Conduct unit and integration testing
- Document customizations

Software Code Promotion/Migration

Custom application objects change management.

- Migration of custom application code/objects from development environments to test environments
- Migration of custom application code/objects from test environments to production environment
- Testing of custom application code/objects
- Management of the testing resources and testing process.
- Software development change control process
- Documentation of software changes

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

600009 Oracle Application Server (iAS) administration

Company's Responsibilities and Included Features

Application Administration

Manage the following areas within the Oracle iAS suite:

- Management and monitoring of Oracle Application Server services including the following components
    - Infrastructure
        - Metadata Repository Schema
        - Oracle Internet Directory
        - Oracle Single Sign-On
        - HTTP Server
    - Middle Tier
        - Forms
        - Reports
        - Portal
        - Discoverer
        - HTTP Server
        - Web Cache

- Cloning environments
- Password management of administrative accounts
- Custom application objects change management. (e.g. Deployment of Forms and Reports files)
- Deployment of OC4J applications (EAR files)
- Configuration and management of data sources
- System configuration file updates as needed relative to break-fix, security, performance or application requirements
- Migration of custom application objects through development, UAT, test, QA environments (as applicable) through to production
- Installation of new Application Server instances
- Routine log file maintenance and purge activity as necessary
- Change control
- Capacity planning
- Troubleshooting and performance tuning

Incident Diagnosis and Troubleshooting

- Diagnosis of system incidents
- Troubleshooting of system incidents
- Engagement of Oracle support
    - Where necessary Company will engage and log service requests with Oracle to rectify software issues
    - Provide client with updates
- Document user issues and system errors

Patching and Upgrades

Break-Fix Patching - Break-fix patch application will follow the incident priority response SLA

- A Break-Fix patch is defined as a patch or series of patches required by Oracle to rectify an error in the application code

Non Break-Fix Patching* - The following are types of patches which are not deemed to be Break-Fix:

- Minor and major version upgrades
- Quarterly Consolidated Patch Upgrade (CPU)
- Maintenance Release

*Requires a 5 business day notification for planning

Patch application is limited to 12 hours per year. Hours exceeding this will be billed on a time and materials basis with prior written approval by the Client

Patch application includes research and installation of Oracle iAS patches, in all iAS instances, by an Oracle Application Admin

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

Development Support

Provide application development resources to develop new or modify existing configurations, extensions, modifications, localizations and integrations

- Develop technical specification based upon functional requirements
- Develop or modify application objects
- Develop or modify reports
- Conduct unit and integration testing
- Document customizations

600011 Oracle BI Publisher application administration

Company's Responsibilities and Included Features

General

Oracle BI Publisher application administration is provided where Oracle BI Publisher is used solely for reporting of Oracle EBS data

- Provide management within the following areas of the application:
  - User security group/role maintenance within the application as defined by the Client
  - Application monitoring
  - Starting, stopping and restarting services.

24x7x365 Help desk support

Incident Triage and Resolution

Company will triage and manage the troubleshooting process for technical system errors.
Company will research problems and issues utilizing:

- Company knowledge of known errors and their solution
- General operating system level troubleshooting
- Escalation to software provider

Resolution of system incidents:

- Application of Company known solutions
- Application of software vendor provided solutions

Engagement of software providers Help Desk support
Document user issues and system errors

Patching and Upgrades

Standard Patch Maintenance - Company shall provide patch application where patches for the application are within the following criteria:

- One-off patches - Patch to address a specific failure to standard functionality (i.e. Break-Fix)
- Any single or group of patches (Service Pack) required to solve a single issue or required by software vendor
- The patching activity is not associated with an application version upgrade

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Development Support

Provide application development resources to develop new or modify existing configurations, extensions, modifications, localizations and integrations

- Develop technical specification based upon functional requirements
- Develop or modify application objects
- Develop or modify reports
- Conduct unit and integration testing
- Document customizations

Database Support

- Provide support for all underlying databases supporting the Oracle BI Publisher application including all data source databases.
- Provide all data ETL design, implement and manage functions.

600012 Oracle Business Intelligence Data Warehouse Administration Console (DAC) Software Support

Company's Responsibilities and Included Features

Incident Triage and Troubleshooting

Company will triage and manage the troubleshooting process for software technical system errors.
Company will research problems and issues utilizing:

- Company knowledge of known errors and their solution
- General operating system level troubleshooting
- Escalation to software provider

Resolution of system incidents through:

- Application of Company known solutions
- Application of software vendor provided solutions
- Engagement of software providers Help Desk support
- Document user issues and system errors

Patching and Upgrades

Standard Patch Maintenance - Company shall provide patch application where patches for the application are within the following criteria:

- One-off patches - Patch to address a specific failure to standard functionality (i.e. Break-Fix)
- Any single or group of patches (Service Pack) required to solve a single issue or required by software vendor

The patching activity is not associated with an application version upgrade

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

User Administration

- Management of user identities within the application:
- User ID adds, deletes and changes
- Security group/role maintenance as applicable to the application as defined by the Client

Job Monitoring and Alerting

- Configuration of transaction error monitoring and email alerting
- Triage and manage the troubleshooting process for transactional and system errors
- Application Notifications can be sent to both Company Support Center and the custome

Data WareHouse Configuration

- Create a physical data model in the data warehouse
- Design subject areas and build execution plans
- Truncating tables
- Managing indexes
- Collecting statistics on tables after the data is populated
- Querying system catalog tables
- Creating the data warehouse schema
- Upgrading, Comparing and Merging DAC Repositories

DAC Application Configuration

- System Configurations
- Database Connectivity
- DAC Server and DAC Repository
- serverSetupPrompt Scripts
- Intergration between DAC and Informatica

Manage metadata driven dependencies and relationships

- Generate and schedule of ETL execution plans
- Capture deleted records
- Manage indexes
- Import \ Export of DAC Metadata
- Perform test runs of execution plans
- Patching of the DAC Metadata
- Move subsets of DAC metadata from one environment to another.

Utilize performance execution techniques

- Automate full and incremental mode optimization rules
- Set the level of ETL session concurrency
- Load balance across multiple ETL servers
- Restart from point of failure
- Create indexes in parallel
- Run appropriate tasks before query indexes have been created
- Queue execution tasks for performance

Development Support

Provide application development resources to develop new or modify existing configurations, extensions, modifications, localizations and integrations

- Develop technical specification based upon functional requirements
- Develop or modify application objects
- Develop or modify reports
- Conduct unit and integration testing
- Document customizations

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

600013 Oracle EBS application administration support

Company's Responsibilities and Included Features

Application Support

Oracle EBS support provides qualified resources to manage Oracle EBS environments within the monthly bucket of hours as contracted.

This includes the following areas within the Oracle EBS:

- Instance management

Cloning environments

- Oracle Workflow
- Notification Mailer
- Concurrent Managers
- Printers and queues
- Password management for Administrators
- Load Balancers

Custom object change management*:

- Migration of customizations through development, test, QA environments (as applicable) through to production
- RICE objects, including package build and deploy
- Change control

24x7x365 Help desk support

* Requires a 5 business day notification for planning.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

600014 Oracle EBS application instance clone

Company's Responsibilities and Included Features

Application Cloning

Application cloning is defined as the process of taking a copy of a environment (usually production) and restoring it to a target environment. This includes both the database and application files.

The Company process involves using the latest or a prior copy of the database hot backup that has already occurred, to restore to the target environment. Live copies of the application files are copied and restored to the target environment.

Company will execute the cloning process on request or on predefined schedules, which can include the following:

- Reconfigure cloned instance to operate in new environment
- Running post-clone scripts
- Validate environment configuration and access
- Notification of completion of clone

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Cloning Request

- Application cloning must be scheduled at least 3 business days in advance.
- Application cloning request must originate from a user approved to request a clone to the target enviroment.
- Users must log out of the target environment prior to scheduled start of clone.

600019 Oracle JD Edwards application administration (CNC) support

Company's Responsibilities and Included Features

Application Support

Oracle JD Edwards CNC support provides qualified resources to manage Oracle JD Edwards environments within the monthly bucket of hours as contracted.

This includes the following areas within the Oracle JD Edwards:

Basic CNC Services:

- Monitor Enterprise One services
- Monitor disk space utilization
- Monitor UBE and other Enterprise One processes
- Monitor and review Enterprise One server logs and incident analysis

Advanced CNC Services:

- Environment and Path code maintenance, including data source and object configuration management
- Cloning environments - Up to one clone per month for each non-production instance or as specified in Line Item Service Boundaries *
- Data and path code refreshes, and environment constructions
- Functional environment troubleshooting and administration to cover Menus, data dictionary, object specifications, and OCM mappings
- Interactive and batch job monitoring and maintenance, to include troubleshooting and incident troubleshooting
- Job scheduler monitoring and scheduler server support
- OMW and Object configuration Management, to include project promotions, transfer rules, PVC administration
- Web forms, and application integrations, and task maintenance
- Default and direct/immediate printer management
- Infrastructure performance monitoring and tuning to support user and process growth
- Oracle Application Server maintenance

Custom object change management:

- Package builds and deployment of customizations through DV, PY, and other environments (as applicable) through to PD
- Object promotions to include version management and menu maintenance
- Change control of package builds, package management and deployments

24x7x365 Help desk support

* Requires a 5 business day notification for planning.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management

- End user client software support

600022 Oracle User Productivity Kit Application Administration

Company's Responsibilities and Included Features

Application User Administration

Management of user identities within the application:

- User ID adds, changes, deletes
- Security group/role maintenance as applicable to the application as defined by the Client

Incident Triage and Resolution

Company will triage and manage the troubleshooting process for technical system errors.
Company will research problems and issues utilizing:

- Company knowledge of known errors and their solution
- General operating system level troubleshooting
- Escalation to software provider

Resolution of system incidents:

- Application of Company known solutions
- Application of software vendor provided solutions

Engagement of software providers Help Desk support
Document user issues and system errors

Patching and Upgrades

Application patching includes research and application of critical updates, recommended patches, updates, and security patches
Break-Fix Patching - Break-Fix patch application will follow the incident priority response SLA
UPK Break-Fix patching is defined as - A patch or series of patches required by Oracle to rectify an error in the application code of Oracle UPK functionality that has already been implemented, tested and is in production in the Client's environment and include any individual patches, dependent patch sets, required to addressed Client specific UPK application issues in functionality that has already been implemented, tested and is in production in the Client's environment, and any Oracle recommended critical CU, Mini-pack or Family-pack needed to address known issues affecting a Client's environment
Non Break-Fix Patching - Non Break-Fix patching requires a 5 business day notification for planning.
The following are types of patches which are not deemed to be Non Break-Fix:

- New functionality
- New architecture
- New modules
- Minor and major version upgrades
- Quarterly Consolidated Patch Upgrade (CPU)
- Maintenance Release
- Family Pack
- Consolidated Update (CU)
- Product Mini-Pack

Major Version Upgrades - Any major version upgrades, will be treated on a time and material basis and shall be planned and billed to Client as agreed upon by the Parties

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

Development Support

Provide application development resources to develop new or modify existing configurations, extensions, modifications, localizations and integrations

- Develop technical specification based upon functional requirements
- Develop or modify application objects
- Develop or modify reports
- Conduct unit and integration testing
- Document customizations

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

600034 EDI Application Support

Company's Responsibilities and Included Features

Gentran EDI Support*

EDI support provides qualified resources to provide supplimental support for a Gentran EDI application. This support can include any of the following areas within Gentran:

- Monitor delinquent functional acknowledgement report and research and resolve any discrepancies received
- Check all email received from EDI translator throughout the day for errors in translation or communication
- Execute monthly archiving of inbound and outbound data (i.e X12 and/or EDIFACT)
- All requests/projects will be required to have a ticket opened for monitoring purposes

Advise Client EDI Manager of issues

- Update ticket as appropriate based on solution or failures or projects
- Mapping changes will require Client approval

Resend EDI documents as appropriate Acknowledge any tickets opened by Company Monitoring tools Ensure successful translation of inbound/outbound EDI documents per Trading Partner requirements Validate all data inbound/outbound has been received/sent successfully via VAN, AS2 or FTP communications General EDI application issue analysis and troubleshooting Assist client in diagnosing or analyzing functional issues as they pertain to EDI
* EDI Support is limited to number of hours per month as shown in Pricing Parameters

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

None

600045 Baan Functional Support

Company's Responsibilities and Included Features

Functional Support*

- Provide functional support in the use of Baan ERP to key and end users
- Triage and troubleshooting functional incidents
- Acting as the Client liaison with software vendors for incident troubleshooting

* Functional support is limited to number of hours per month as contracted

Support Prioritization

Support requests will be prioritized as follows:
First Level - To support the Client s Baan ERP users with questions and issue resolution as defined through trouble tickets administered by Company s Support Center
Second Level - To participate in the functional design and testing of customizations to Baan ERP, as defined by Client

Third Level - To participate in any additional projects or initiatives required by Client

Functional support is provided during the business hours of 6:00 AM PDT to 3:00 PM PDT, Monday through Friday, excluding normal Client holidays.

Functional Support Hours Management

- For any Baan ERP functional issues raised by Client, Company shall work to resolve each such issue for up to four (4) hours
- Upon reaching the four-hour limit for any one issue, Company shall contact Client to receive approval to continue the proposed troubleshooting
- Company shall provide a monthly report on hours consumed
- Client approved functional support hours spent in excess of allocated hours shall be provided on a time and materials basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Screening Functional Issues

- Client shall internally review each functional issue and determine the necessity of escalating such issue to Company.

This is done to limit unnecessary use of allocated functional support hours

Baan ERP Development

- Code development
- Report development
- Code troubleshooting and maintenance

600119 File Transfer Services (FTP) administration

Company's Responsibilities and Included Features

FTP Application/Site Management

- FTP server availability monitoring and management
- Global FTP settings management against Company s best practices
- FTP permissions management
- Log maintenance
- Advanced system administration support for FTP infrastructure issues

Incident Triage and Resolution

Company will triage and manage the troubleshooting process for technical system errors.
Company will research problems and issues utilizing:

- Company knowledge of known errors and their solution
- General operating system level troubleshooting
- Escalation to software provider

Resolution of system incidents:

- Application of Company known solutions
- Application of software vendor provided solutions

Engagement of software providers Help Desk support
Document user issues and system errors

Patching and Upgrades

Standard Patch Maintenance - Company shall provide patch application where patches for the application are within the following criteria:

- One-off patches - Patch to address a specific failure to standard functionality (i.e. Break-Fix)
- Any single or group of patches (Service Pack) required to solve a single issue or required by software vendor
- The patching activity is not associated with an application version upgrade

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

600120 Microsoft IIS Administration

Company's Responsibilities and Included Features

Web Health Monitoring

Monitoring and review of:

- Windows event logs
- IIS logs
- IIS services
- FTP Publishing Service
- World Wide Web publishing Service

Web System Administration

Manage the following areas within IIS:

- IIS services availability and reliability
- Performance Tuning
- Creation or Extending of Web Applications
- Creation, and management of directories and their properties
- Managing Windows security
- External site availability, redirects and SSL management (if applicable)
- Site creation and maintenance delegation to expert contacts as defined by Client
- Certificate creation and management

Patch Management

- Periodic review of critical patches in collaboration with underlying OS administrator
- Up to quarterly routine review same version patch analysis and application
- Application of updates and patches during approved maintenance windows

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client

staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Web Content Management

- Creation of new sites within a site collection
- Application development, customization and maintenance
- User management
- Third-party Application Dependencies

600122 Microsoft Exchange Administration

Company's Responsibilities and Included Features

Mailbox Administration

- Managing User accounts and Mail Features
- Managing Contacts
- Managing Distribution List
- Managing Offline Address Books
- Managing Online Address Lists
- Managing Mailboxes
- Configuring Mailbox Delivery Restrictions, Permissions, and Storage Limits

Managing Databases and Storage Groups

- Creating and Managing Database Availability Groups
- Managing Mailbox and public Folder Databases

Managing Web and Mobile Access

- SSL Certificate management
- Configuring Outlook Anywhere / RPC over HTTPS
- Configuring POP3 and IMAP4
- Managing Exchange Server Features for Mobile Devices

Administering permissions, rules, policies, and security settings

- Configuring Standard Permissions for Exchange Server
- Configuring Role-Based Permissions for Exchange Server
- Auditing Exchange Server Usage
- Configuring Compliance and Messaging Retention
- Configuring Standard Permissions for Exchange Server
- Configuring Role-Based Permissions for Exchange Server

Messaging Policy and Compliance Management

- Configuring transport rules
- Configuring and managing journaling

- Configuring and managing archiving

Optimizing message processing, logging, and anti-spam filtering

- Working with SMTP Connectors, Sites, and Links
- Managing Message Pickup, Replay, Throttling, and Back Pressure
- Creating and Managing Accepted Domains
- Creating and Managing E-Mail Address Policies
- Creating and Managing Remote Domains
- Configuring Anti-Spam and Message Filtering Options

System Maintenance, Monitoring, and Queuing

Monitoring and rectifying issues in the following system areas:

- Services
- Resource usage
- Queues

Backup and Restore Management

- Monitoring Backups
- Manage mailbox/database restores (Limited to number of restores as listed in Pricing Parameters Parameters)

Upgrade and Patch Management

- Periodic review of critical patches
- Up to quarterly routine review same version patch analysis and application
- Application of same version updates and patches during approved maintenance windows
- Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

End User Support and Management

Support of end users

- Application functional support
- Content or data related support
- Email client support

600125 Microsoft Remote Desktop (RDS) Administration

Company's Responsibilities and Included Features

Application Administration

Manage the following areas within Microsoft Remote Desktop Services (RDS):

- Policy management
- RDS license management (on server)
- RDS gateway management (if exists; for public Terminal Services)
- RDS application publication
- RDS settings management against Company s best practices
- Permissions structure and definitions per Client specifications
- Log maintenance
- Advanced system administration support for RDS infrastructure issues
- Application of RDS delivered application patches where administrator level access is required. This will be applied under direction of the delivered application administrator

24x7x365 Help desk support

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Engagement of software providers Help Desk support (requires Client to have a support contract with the software provider)
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues
- Provide client with updates

Document user issues and system errors

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

End User Support and Management

- Support of non-super users
- Application functional support

- Content or data related support or management
- End user client software support

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Remote Desktop Services Delivered Application Support

- Functional and technical support of applications delivered by RDS
- RDP client support

600126 Microsoft Active Directory Services Administration (Standard)

Company's Responsibilities and Included Features

Single Domain Forest Administration

Provide Microsoft Active Directory (AD) administration of a single forest, single domain including administration, design and implementation of:

- Local DNS configurations
- AD sites and subnets definition
    - Creation of site(s)
    - Creation of AD replication topology
    - Creation of inter-site connectors
    - Creation of subnets and assigned-to site(s)
- OU Container Structure
- Logon scripts (Limited to printer and drive mapping)
- Group policy objects
- FSMO role administration
- Global Catalog placement/removal
- Security groups / Distribution groups
- Delegation of administrative roles
- Domain controller promotions
- Domain controller demotions
- Removal of AD roles (FSMO or GC)
- Removal of domain controller object from sites, and subnets

Domain Admin/Enterprise Admin access is limited to Company

DHCP Administration

- Modify or deletion of existing scopes
- Add, modify, or deletion of reservations (usually done on subnet and then applied to each associated scope)

Compliance Reporting and Auditing (If compliance reporting indicated in Pricing Parameters)

Collection and reporting on Active Directory regulatory requirements, including:

- User counts
- Disabled/inactive accounts
- Password policy
- Group membership
- Built-In administrative group auditing

Domain User Administration

Provisioning of Active Directory domain users:

- Group membership updates
- Password resets
- Termination of AD domain users
- No change notice is required for User Administration

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

End User Support

24 x 7 End User helpdesk support related to:

- Password resets
- Account lockout resets

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating System (OS) Administration

- Provide OS administration of the server/s on which AD is being managed. Company provided OS administration is available under a separate ItemID.
- Providing Domain access to AD to Company administrators
- Ensuring that OS security patching is no more than 90 days out of date if Client has not contracted for Company provided OS administration

Active Directory Policy

Define Active Directory domain policies including:

- User naming standards
- Group policies
- Account password policy
- Account lockout policy
- User add/change/delete policy
- Security policies

Advanced User Identity/Credential Management:

Administration of advanced identity or credential management systems including:

- Biometric identities
- Smart cards
- RSA tokens
- Microsoft MFA

- Other 3rd-party MFA solutions

600159 Microsoft Active Directory Services Administration (Child Domain)

Company's Responsibilities and Included Features

Single Domain (Child)

System administration of a Child Domain including:

- Local DNS configurations
- Design/Implement Active Directory roles (FSMO/GC placement)
- AD Sites and Subnets definition
- Creation of Site(s)
- Creation of AD Replication Topology
- Creation of Inter-Site Connectors
- Creation of Subnets and Assigned to site(s)

Design/Implement - OU Container Structure Develop/Implement - logon scripts (Limited to printer and drive mapping) Implement - Group Policy Objects Develop/implement Security groups / Distribution groups Delegation of administrative roles Domain Controller promotions Domain Controller demotions Removal of Active Directory roles (FSMO or GC) Removal of domain controller object from Sites and Subnets Domain Admins

Active Directory Reporting

- Reporting of user counts
- Disabled/inactive accounts

Compliance Reporting and Auditing (If compliance reporting indicated in Pricing Parameters)

Collection and reporting on Active Directory regulatory requirements, including:

- Password policy
- Group membership
- Built In administrative group auditing

Domain User Administration

Provisioning of Active Directory domain users:

- Group Membership Updates
- Password resets
- Termination of Active Directory domain users
- No change notice required for User Administration

End User Support

24 x 7 End User helpdesk support related to:

- Password resets
- Account lockout resets

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Active Directory Policy

Define Active Directory domain policy including:

- User naming standards
- Account password policy
- Account Lockout policy
- User add/change/delete policy
- Security policies

Advanced User Identity/Credential Management:

Administration of advanced identity or credential managements system, i.e:

- Biometric identities
- Smart cards
- RSA tokens

600160 Microsoft Active Directory Services Administration (Resource Domain)

Company's Responsibilities and Included Features

Trusted Domain (Resource)

System administration of a Resource Domain including:

- Local DNS configurations
- Design/Implement Active Directory roles (FSMO/GC placement)
- AD Sites and Subnets definition
- Creation of Site(s)
- Creation of AD Replication Topology
- Creation of Inter-Site Connectors
- Creation of Subnets and Assigned to site(s)

Design/Implement - OU Container Structure Develop/Implement - logon scripts (Limited to printer and drive mapping) Implement - Group Policy Objects Develop/implement Security groups / Distribution groups Delegation of administrative roles Domain Controller promotions Domain Controller demotions Removal of Active Directory roles (FSMO or GC) Removal of domain controller object from Sites and Subnets Domain Admins/Enterprise Admins access is limited to Company

Active Directory Reporting

- Reporting of user counts
- Disabled/inactive accounts

Compliance Reporting and Auditing (If compliance reporting indicated in Pricing Parameters)

Collection and reporting on Active Directory regulatory requirements, including:

- Password policy
- Group membership
- Built In administrative group auditing

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Active Directory Policy

Define Active Directory domain policy including:

- User naming standards
- Account password policy
- Account Lockout policy
- User add/change/delete policy
- Security policies

Advanced User Identity/Credential Management:

Administration of advanced identity or credential managements system, i.e:

- Biometric identities
- Smart cards
- RSA tokens

End User Account Management and Support

End users to managed in Client's primary domain not in this Resource Domain:

- Provisioning of Active Directory domain users
- Group Membership Updates
- Termination of Active Directory domain users
- End User support related to:
- Password resets
- Account lockout resets

600163 Dedicated Backup Infrastructure and Software Administration

Company's Responsibilities and Included Features

Backup Management Console Server Administration

- Configuration of Backup Policies
- Monitoring and Reporting of backup status
- Rectification and resubmission of failed backup jobs if appropriate

Tape Management (as required)

- Physical tape handling
- Off-Site tape storage

Hardware Maintenance Management

Manage hardware replacement and or repair with hardware vendor

- Perform analysis of any hardware additions or upgrades
- Apply hardware BIOS updates as necessary

System Administration
System administration of the server operating system including:

- Operating system configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks

System Patch Management

- Periodic review of backup software and operating system updates (Critical/Important/Security)
- Review of updates to be applied to server(s) and software
- Change notice submission, approval and application of updates

Major or Point Release Upgrades.

- Periodic next version upgrade analysis and recommendations
- Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

System Incident Diagnosis and Resolution

- Document issues and system errors
- Diagnosis of system incidents
- Troubleshooting of system incidents

System Administration Documentation

- Document applicable hardware and system administration procedures and policies

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Backup Infrastructure

- Backup appliance or server hardware to enable backup to disk and/or tape
- Available disk storage and tape media as required
- Procurement of current hardware support and maintenance

Backup Software Licensing

- Procurement of backup software (server and agent) licensing for current version on current operating system
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Backup Policy Definition

Client is responsible for defining:

- What must be backed up?
- When and how often it must be backed up
- How it must be backed up. (Full, Incremental, Differential)
- Local backup retention policy
- Archive tape content, timing and retention policy

600164 Citrix Server Application Administration

Company's Responsibilities and Included Features

Citrix System Administration

- Citrix services availability and reliability management
- Citrix Configuration
- Citrix Security Configuration
- Citrix load balancing management (if applicable)
- Installation of printer drivers to support Citrix supported business class printers
- Advanced system administration support for Citrix infrastructure issues
- License Server Management

Citrix Health Check Monitoring

Monitoring and review of:

- Citrix service availability
- Citrix application delivery availability
- Citrix portal availability

Citrix Patch Management

- Periodic review of critical patches
- Up to quarterly routine review same version patch analysis and application
- Application of updates and patches during approved maintenance windows

Application Software Management

Support of applications loaded on the Citrix servers will be limited to:

- Application of software patches in collaboration with the Application System Administrator

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Application Support

Support in the following areas of the applications loaded onto Citrix:

- Functional Support
- Configuration of the application from within the application
- Application issue triage and resolution
- Patch Identification
- Application Installation (will be supported by Company under T and M projects)
- Application Upgrades (will be supported by Company under T and M projects)
- End User Support

600166 Microsoft Windows File Services Administration

Company's Responsibilities and Included Features

File services management

Permissions Management:

- Add/Remove Active Directory groups to folders.

Folder Management:

- Add/Remove Folders

Storage Monitoring:

- Monitor disk space usage.

Distributed File System (DFS) management (if included):

- Add remove servers from DFS
- Monitor and maintain DFS replication

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

File Systems Permissions Management

Define permission strategy, including:

- Group Naming Convention
- Group membership approval
- Level of permission approval

Folder Management

Define folder structure, including:

Folder naming convention

- Folder hierarchy

Storage Utilization
Determine files that can be compressed or deleted as needed.

Backup Infrastructure (Tape or Disk based)
Backup system to enable backup of data from this server to tape or disk, including:

- Backup server and agent licensing
- Available disk storage and tape media if required

OR
Contracted usage of the Company Backup service

600168 Microsoft Office Communication Server administration (IM/meeting services only)

Company's Responsibilities and Included Features

Application Administration
Administration and support of the application for instant messaging (IM) and meetings in the following areas :

- User and security management (requires independent Active Directory management)
- Managing on-premises meeting configuration
- Server infrastructure configuration and support
- Federation configuration and support
- Public IM access configuration and support
- Global setting configuration and maintenance
- Configuring server side support for clients and devices
- Services and log monitoring

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Engagement of software providers Help Desk support (requires Client to have a support contract with the software provider)
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues
- Provide client with updates

Document user issues and system errors

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Patching and Upgrades
Standard Patch Maintenance - Company shall provide patch application where patches for the application are within the following criteria:

- One-off patches - Patch to address a specific failure to standard functionality (i.e. Break-Fix)
- Any single or group of patches (Service Pack) required to solve a single issue or required by software vendor
- The patching activity is not associated with an application version upgrade

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

Enterprise Voice Administration
Administration and support of the following additional Enterprise Voice application areas:

- Configure and management of voice routing
- Configure and management of incoming call handling features
- Configure and management of response groups
- Configure and management of external connectivity and communications

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Archive and Call Monitoring Management
Administration and support of the following additional application functionality:

- Call monitoring
- Communication archiving

600172 Microsoft Windows Print Services Administration

Company's Responsibilities and Included Features

Print services management
Permissions management:

- Add/Remove Active Directory groups to printer queues.

Server printer device driver management:

- Install new drivers
- Update drivers

Printer device queue management:

Setup new printer queues

- Restart printer queues

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Printer hardware support

Maintenance of printer:

- Cleaning
- Paper jamming rectification
- Replacement of consumables
- Repair of printer

Installation and connection of printer
Printer hardware troubleshooting

Printer software support

Configuration of printer
Installation of desktop printer software and drivers
Printer software troubleshooting

End User Support

- Support of non-expert OS users (Typically refers to non-IT department staff or application end users)

600181 Dedicated Remote Backup Infrastructure and Software Administration

Company's Responsibilities and Included Features

Backup Management Console Server Administration

- Configuration of Backup Policies
- Monitoring and Reporting of backup status
- Rectification and resubmission of failed backup jobs if appropriate

Hardware Maintenance Management

- Manage hardware replacement and or repair with hardware vendor
- Perform analysis of any hardware additions or upgrades
- Apply hardware BIOS updates as necessary

System Administration

System administration of the backup console and or media server operating systems including:

- Operating system configuration

- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks

System Patch Management

- Periodic review of backup software and console/media server operating system updates (Critical/Important/Security)
- Review of updates to be applied to server(s) and software
- Change notice submission, approval and application of updates

Major or Point Release Upgrades.

- Periodic next version upgrade analysis and recommendations
- Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

System Incident Diagnosis and Resolution

- Document issues and system errors
- Diagnosis of system incidents
- Troubleshooting of system incidents

System Administration Documentation

- Document applicable hardware and system administration procedures and policies

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Backup Infrastructure

- Backup appliance or server hardware to enable backup to disk and/or tape
- Available disk storage and tape media as required
- Procurement of current hardware support and maintenance

Backup Software Licensing

- Procurement of backup software (server and agent) licensing for current version on current operating system
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Backup Policy Definition

Client is responsible for defining:

- What must be backed up?
- When and how often it must be backed up
- How it must be backed up. (Full, Incremental, Differential)
- Local backup retention policy
- Archive tape content, timing and retention policy

Backup Source Server Management
Management of server being backup up, including:

- Installation, patching and upgrades of backup agents on server being backed up
- Local configuration of backup agent and exclude lists on server being backed up
- Management of restores

Tape Management (as required)

- Physical tape handling
- Off-Site tape storage

600314 Oracle Technical Architect Support

Company's Responsibilities and Included Features

Oracle Technical Architect Support*

* Oracle Technical Architect Support is limited to number of hours per month as contracted.

Company will provide the following services to support Client s development, functional and management teams:

- Support of existing Client s Oracle environments, including integration, third party systems, network configuration, and environment infrastructure
- Collaboration with Oracle EBS business, functional, and development teams and their requirement
- Periodic review of Oracle EBS solution configuration, health, and performance, including systems, applications, BI, and databases
- Recommendations on Oracle EBS solution roadmap including minor (dot) releases for RUP, PSU and CPU
- Recommendations on Oracle EBS solution security setup, familiarity with OIM & AD integration
- Oracle EBS & Database security analysis and work with the auditors

Service Delivery

- Services will be available 9:00am to 5:00pm EDT Monday to Friday excluding Company holidays
- Service requests are to be requested through the Company Help Desk
- Unconsumed hours for the month will not roll over to the next month

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

None

600481 Third Party Solution - Backup Management

Company's Responsibilities and Included Features

This service is provided as an add on to item 600476-Help Desk and User Support and provides support of Client's backup system.

Backup System Support:

- Manage existing backup jobs

- Adjust backup configurations upon client request or to adjust to issues
- Coordinate maintenance with Client contracted support provider

Item 600476-Help Desk and User Support is required for this service.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Managing the server and operating system on which the backup system operates
- Maintenance of the underlying infrastructure on which the backup system operates

600508 Volume Discount - Level 1

Company's Responsibilities and Included Features

Company agrees to discount each month's Monthly Fees by the amount shown in the Monthly Fees for this ItemID, if the total SOW's Monthly Fees, including actual metered services fees are in excess of One Hundred Ten Thousand Dollars ($110,000.00)

600509 Volume Discount - Level 2

Company's Responsibilities and Included Features

Company agrees to discount each month's Monthly Fees by the amount shown in the Monthly Fees for this ItemID, if the total SOW's Monthly Fees, including actual metered services fees are in excess of One Hundred Ten Thousand Dollars ($140,000.00)

600510 Standard SLA Acceptance Discount

Company's Responsibilities and Included Features

Company agrees to discount each month's Monthly Fees by the amount shown in the Monthly Fees for this ItemID as Client has accepted the standard SLA as documented in this SOW

600644 XenApp Management

Company's Responsibilities and Included Features

- XenApp application delivery services management
- Access gateway management
- Web interface management
- Application package publishing management
- Shared published desktop management
- User rights administration
- Policy management
- Printer driver management
- XenApp application patching

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- End user device management
- Printer device management
- End user support
- Application Package and management
- Desktop image & management
- Server hardware
- Application dependencies

,2.8,2.8,4.0,0.0%,4.0,4.0,30.0%, 148

601260 Microsoft Windows Server Update Services Administration

Company's Responsibilities and Included Features

Windows Server Update Services (WSUS) Administration

- Configure update synchronization based on product family
- Download Microsoft Windows update to the WSUS server
- Distribute the Microsoft Windows updates to the Client s servers and desktops
- Manage computer groups
- Manage WSUS group policies
- Approve and decline updates

Windows Server Update Services Administration is limited to the number of hours per month as contracted. Unconsumed support hours will not be rolled over to the next month.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- WSUS server contracted for Company provided operating system managed services
- Configuration of Client's desktops patch update settings
- Configuration of Client's servers patch update settings
- Remediation of Client's desktop's failed updates
- Remediation of Client's server's failed updates

601270 Production Faxing Application Solution

Company's Responsibilities and Included Features

The following components comprise a customized faxing application that is hosted and managed by Company.

- Hosting infrastructure
- Router/voice gateway managed services
- PSTN and voice connectivity services
- Xmedius fax software management
- EDM FAX software license and management

Hosting Infrastructure Managed Dedicated Router / Voice Gateway

Ln#	Qty	Item	Description
1	1	Primary Router	Cisco 2901 or equivalent. 2 Port PRI card and 2 Port POTS/Analog modem
2	1	Secondary Router	Cisco 2901 or equivalent. 2 Port PRI card and 2 Port POTS/Analog modem

- Managed Dedicated Router SLA
  - The service level of availability (SLA) is 99.95%
- Repair Service level objective
  - The Service Level Objective (SLO) for repair or replacement is next business day or better.

- Management Responsibilities
  - Management of interface IP addresses
  - Configuration of routing protocols (Static, RIP, EIGRP, OSPF, etc.)
  - IP interface availability monitoring and performance reporting
  - NTP service management
  - Monitor circuits for up/down status
  - Report on circuit bandwidth utilization via monitoring on managed router

- Error and discard reporting
- Identify outages and escalate to circuit vendor by opening trouble ticket
- Escalate trouble tickets with vendor following Company standard operating procedure

PSTN and Voice Connectivity Services

Ln#	Qty	Service Type	Description
1	1	T1/PRI	Primary path PRI
2	1	T1/PRI	Secondary path PRI
3	4	Analog line	POTS Analog line for Fax/Modem use
4	1	DID Number block	100 Direct Inward Dialing numbers with forward to Business Continuity location

Xmedius Fax Software

Software Management

- Troubleshoot incoming/outgoing fax failures. FFailure must be identified by local resource as not being due to user error or circuit unavailability/congestion.
- Troubleshoot system-related issues impacting fax server operation (fax manager, fax drivers and rasterization services).
- Troubleshoot fax client issues.
- Troubleshoot client issues.
- Configuration Management fax for minor configuration-related tasks.
    - Minor changes are defined as those that take two hours or less to plan, implement and test, collectively. Major changes will be billed on a time and materials basis in addition to the monthly service fee for Management. Additional configuration and administration changes are also available on a time and materials basis.

EDM FAX Software License

Provide Anju Technology, LLC, EDM FAX Software DocX Online product DoRs

- Bundled Server License
- Software License for 150 users
- Upgrades to new versions

DoRs Application Management

- Ongoing Management of EDM FAX (DoRs) Application
- Monitoring of the DoRs application database for performance and maintenance
- Review of error logs for proactive response to any potential issues.
- Tier III support: bug fixes and analysis of reported issues
- Product subject matter expertise
- Upgrade to new versions. Requires 3 (three) months notice to upgrade.

Custom Development

Application support, modifications and customization are provided by third party Anju Technology LLC. Customized development will be billed as time and materials as scoped service request / change order.

- Maintain contract with Anju support services
- Work with Client to define customization or service modifications
- Coordinate work to be completed from Anju Technologies with Company change control processes.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating system software licensing

- Procurement of OS software and licensing for current version of operating system, including any user access licensing
- Providing software media for installation
- Procurement of current software maintenance where applicable

Xmedius software licensing

- Procurement of OS software and licensing for current version of operating system, including any user access licensing
- Providing software media for installation
- Procurement of current software maintenance where applicable

Contract for Company supporting services

- Cross-connections for T1/PRI circuits and analog POTS lines
- ReliaCloud Integration cabinet services to house the managed dedicated routers
- ReliaCloud Integration 1 Gbps LAN connections (2) to each managed dedicated router

End user support

- Support of non-expert OS users (Typically refers to non-IT department staff or application end users)

601271 Disaster Recovery Faxing Application Solution

Company's Responsibilities and Included Features

The following components comprise a customized faxing application that is hosted and managed by Company.

- Disaster Recovery Hosting infrastructure
- Router/voice gateway managed services
- PSTN and voice connectivity services
- Xmedius fax software management
- EDM FAX software license and management

Hosting Infrastructure Managed Dedicated Router / Voice Gateway

Ln#	Qty	Item	Description
1	1	DR Router	Cisco 2901 or equivalent. 2 Port PRI card and 2 Port POTS/Analog modem

- Managed Dedicated Router SLA
  - The service level of availability (SLA) is 99.95%
- Repair Service level objective
  - The Service Level Objective (SLO) for repair or replacement is next business day or better.

- Management Responsibilities
  - Management of interface IP addresses
  - Configuration of routing protocols (Static, RIP, EIGRP, OSPF, etc.)
  - IP interface availability monitoring and performance reporting
  - NTP service management
  - Monitor circuits for up/down status
  - Report on circuit bandwidth utilization via monitoring on managed router
  - Error and discard reporting
  - Identify outages and escalate to circuit vendor by opening trouble ticket
  - Escalate trouble tickets with vendor following Company standard operating procedure

PSTN and Voice Connectivity Services

Ln#	Qty	Service Type	Description

1	1	T1/PRI	Primary path PRI
2	1	Caller ID	Caller ID for EDP

Xmedius Fax Software

Software Management

- Troubleshoot incoming/outgoing fax failures. Failure must be identified by local resource as not being due to user error or circuit unavailability/congestion.
- Troubleshoot system-related issues impacting fax server operation (fax manager, fax drivers and rasterization services).
- Troubleshoot fax client issues.
- Troubleshoot client issues.
- Configuration Management fax for minor configuration-related tasks.
    - Minor changes are defined as those that take two hours or less to plan, implement and test, collectively. Major changes will be billed on a time and materials basis in addition to the monthly service fee for Management. Additional configuration and administration changes are also available on a time and materials basis.

EDM FAX Software License

Provide Anju Technology, LLC, EDM FAX Software DocX Online product DoRs

- Bundled Server License
- Software License for 150 users
- Upgrades to new versions

DoRs Application Management

- Ongoing Management of EDM FAX (DoRs) Application
- Monitoring of the DoRs application database for performance and maintenance
- Review of error logs for proactive response to any potential issues.
- Tier III support: bug fixes and analysis of reported issues
- Product subject matter expertise
- Upgrade to new versions. Requires 3 (three) months notice to upgrade.

Custom Development

Application support, modifications and customization are provided by third party Anju Technology LLC. Customized development will be billed as time and materials as scoped service request / change order.

- Maintain contract with Anju support services
- Work with Client to define customization or service modifications
- Coordinate work to be completed from Anju Technologies with Company change control processes.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating system software licensing

- Procurement of OS software and licensing for current version of operating system, including any user access licensing
- Providing software media for installation
- Procurement of current software maintenance where applicable

Xmedius software licensing

- Procurement of OS software and licensing for current version of operating system, including any user access licensing
- Providing software media for installation
- Procurement of current software maintenance where applicable

Contract for Company supporting services

- Cross-connections for T1/PRI circuits
- ReliaCloud Integration cabinet services to house the managed dedicated routers
- ReliaCloud Integration 1 Gbps LAN connections (2) to each managed dedicated router

End user support

- Support of non-expert OS users (Typically refers to non-IT department staff or application end users)

601449

Company's Responsibilities and Included Features

Company will provide support of Client s banking scripts used to push or pull data to or from Client s banking institutions as described below.

Banking Script Support

- Troubleshoot existing scripts
- Re-run scripts on request
- Modify existing scripts to rectify data transfer failures where applicable
- Create directories in specified locations
- Password management for scripts within what is used or stored by the banking script system
- File retrieval and restore to an alternate location
- Script run schedule management
- Manage email alert notifications
- Banking script support is limited to managing up to 120 actively running scripts
    - The script count is based upon individual tasks the scripts are executing
    - Examples of script tasks are:
        - Pull 1 file
        - Push 1 file
        - Generate emails
        - Test connection
        - Rotate Logs

New Banking Script Development

- Review and validate new banking script requirements as provided by Client
- Develop script
- Test and validate the script in conjunction with the Client is working as designed
- The development of new banking scripts is limited to 6 new scripts per contract year

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Facilitate and be present in all communications with the Client s banks
- Provide documented requirements for new scripts

601465

Company's Responsibilities and Included Features

Techno-Functional Support*

- Provide Techno-Functional (TF) support for the following Oracle applications as listed in Client s BID 2019-22:
    - ITEM 1 PROGRAMMER/2000 V7.2 - CSI #1732889 (QTY 3)
    - ITEM 2 DEVELOPER/2000 1.3 - CSI #1732903 (QTY 2)

- ITEM 13 Oracle Internet Developer Suite Named User Perpetual CSI #13553707 (QTY 2)
- ITEM 15 Oracle Internet Developer Suite Named User Plus Perpetual CSI #18061628 (QTY 4)
- ITEM 16 Oracle WebLogic Suite Processor Perpetual CSI #18061628 (QTY 3)
- ITEM 17 Oracle WebLogic Suite Processor Perpetual CSI #18061628 (QTY 1)
- ITEM 18 Oracle Business Intelligence Server Administrator Named User Plus Perpetual CSI #16497171 (QTY 2)
- ITEM 19 Oracle Business Intelligence Suite Enterprise Edition Plus Named User Plus Perpetual CSI #16497171 (QTY 50)

Troubleshoot and diagnose technical incidents

- Perform Oracle patch impact analysis
- Work with the business on day-day data fixes
- Perform root cause analysis (RCA) for critical and repetitive incidents on request
- Coordinate TF incidents with Company technical administration team and 3rd party vendors, including Oracle
- Communicate TF support status to the Client's leadership team
- Act as the Client liaison with software vendors for incident troubleshooting
- Participate in the functional design and testing of customizations to Oracle EBS, as defined by Client
- Company assumes that the information provided during TF discussions and through documents is accurate and up-to-date. Result of incorrect information can result in risk to business systems stability and data integrity and could result in support hours being consumed for rework
- Workaround(s) to production bugs will be suggested by Company team only if they are supported by Oracle
- For any TF or development issues raised by Client, Company shall work each such issue for up to four (4) hours, upon reaching the four-hour limit for any one issue, Company shall contact Client to receive approval to continue the proposed troubleshooting
- Oracle CSR resolution is dependent on the solutions or fixes from Oracle Corporation
- Company assumes that the Client's business users will be available for any discussion required for problem troubleshooting and resolution and will be provided in a timely manner
- All incidents and requests will be logged and managed through Client provided incident management system

TF support is provided by non-USA resident resources (offshore)

* TF support is limited to the number of hours per month as contracted for this ItemID. Unused hours will not roll over to subsequent months.

TF Support Prioritization and Engagement Objectives

- Company will provide support to the Client s Oracle EBS users for TF support through question and issue submission through incident tickets submitted to and administered by Company s help desk, prioritized as follows:

Priority	Definition	Support Hours	Engagement Objective during Support Hours
1	One or more business critical application functions is impeding the customer s ability to perform business.	Monday-Friday, 8am-5pm CST/CDT	30 minutes
2	One or more business critical application functions are degraded and is impacting the customer s ability to perform business.	Monday-Friday, 8am-5pm CST/CDT	2 hours
3	The incident has a medium impact on the customer's ability to perform business.	Monday-Friday, 8am-5pm CST/CDT	4 hours
4	The incident has a minor impact on the customer's ability to perform business.	Monday-Friday, 8am-5pm CST/CDT	24 hours
5	The incident has no impact to the customer s ability to perform business.	Monday-Friday, 8am-5pm CST/CDT	48 hours

- TF support will be provided on a best-effort basis for any time outside of the designated support hours unless agreed upon in advance by both parties

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Screening Functional Issues
  - Client shall internally review each functional issue and determine the necessity of escalating such issue to Company. This is done to limit unnecessary use of allocated support hours
- Oracle EBS Development
  - Code Development
  - Report Development
  - Code troubleshooting and maintenance
- A current Oracle application software support agreement with the software provider or alternate 3rd party provider must be in place
- Necessary software licensing to enable functional support staff to access Client systems

601517

Microsoft Office 365 User Provisioning Administration provides move, add, change, delete services for managing the assignment of Microsoft Office 365 licenses to users and provisioning Microsoft Office 365 end user features on behalf of Client.

Company's Responsibilities and Included Features

User Management

- Add, edit, remove users either through:
  - Microsoft 365 admin center
  - Client s local Active Directory (AD) that is being synchronized to Azure AD
- Assign, reassign and unassign Office 365 licenses to users
- Manage user mailbox settings
- Manage user audio conference settings for Microsoft Teams

Group and Resource Management

- Manage groups and resources by adding, editing, and/or deleting:
  - Security groups
  - Distribution lists
  - Mail-enabled security groups
  - Contacts
  - Shared mailboxes
  - Rooms and equipment
  - Calendar sharing

Mobile Device Access

- Manage mobile devices by adding, editing, and/or deleting:
  - Quarantined devices and device access rules
  - Mobile device mailbox policies and device access rules

Public Folders

- Manage public folders by adding, editing, and/or deleting:
  - Public folders
  - Public folder mailboxes

Service Metering

- This is a metered service.
- The Service is billed as percentage of the Client s monthly Microsoft Office 365 product license usage at Microsoft s list price. This is quoted as a rate per US Dollar of licensing consumed.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Client must obtain the Office 365 subscription(s) to be managed by Company through Company s Microsoft Cloud Service Provider program
- Identify named Client users authorized to make requests for Office 365 provisioning and changes
- Provide Company with administrative credentials within the Office 365 domain to be managed
- Areas of Office 365 provisioning not included in services scope:
  - Office 365 Security and Compliance management
  - Setup or reconfiguration of any non-user specific or global feature, policy or functionality
  - Unified messaging
  - SharePoint site provisioning
  - SharePoint site user access permissions
- End-user desktop provisioning and support
- End-user support
- Local AD administration
- Microsoft Azure AD connect management

601518

Company's Responsibilities and Included Features

Microsoft Office 365 Technical Support provides technical support of a Client s Microsoft Office 365 environment as provided below:

Office 365 Technical Incident Triage and Troubleshooting

- Triage of Office 365 incidents
- Troubleshoot and work to resolve Office 365 incidents

Office 365 Configuration

- Advise Client on Office 365 configuration
- Add, edit, remove, adjust Office 365 configurations to complement Client s business requirements
- Support of integration aspects of Office 365 as integrated with an on-premise Microsoft Exchange environment (commonly called an Office 365 hybrid environment) is only included if the Company is contracted to manage Client s on-premise Microsoft Exchange environment

Designated Contact Technical Support*

Technical support may only be requested by Client Designated Contacts*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* A Designated Contact is defined as someone who is authorized by Client to request support or changes be made to the configuration of the Client s Office 365 environment. The number of Designated Contacts is limited to 5 or 5% of the Client staff, whichever is greater.

Service Metering

- This is a metered service.
- The service is billed as percentage of the Client s monthly Microsoft Office 365 product license usage at Microsoft s list price. This is quoted as a rate per US Dollar of licensing consumed.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Client must obtain the Office 365 subscription(s) to be managed by Company through Company s Microsoft Cloud

Service Provider program
- New Microsoft Office 365 environment initial setup and configuration.
- Office 365 migration support
- Identify Client Designated Contacts
- Provide Company with administrative credentials within the Office 365 domain to be managed
- Day to day Office 365 end user provisioning
- Unified messaging configuration
- Teams telephony integration
- SharePoint site provisioning
- SharePoint site user access permissions
- End-user desktop provisioning and support
- End-user support

Security and Compliance

- Local Active Directory (AD) administration
- Azure AD connect, Active Directory Federation Services (ADFS) management
- Multi-factor authentication (MFA) support
- Office 365 Security and Compliance management

601684 VMware Horizon Standard Edition Administration

Definitions

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services.

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged cluster.

Company's Responsibilities and Included Features

OneNeck will provide basic management for Horizon View Standard Edition. This service is delivered per Node within the Cluster that delivers Vmware Horizon services.

Service Metering Management

- Company management of Horizon View usage meter
- Consumption based reporting to Vmware on software usage

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Subscribe to VMware Horizon Standard Edition Administration for each Node within the Cluster that delivers Vmware Horizon services.
- Subscription to Company VMware Horizon Standard Edition licensing is required
- Subscription to a Company VMware ESXi managed services is required

Client must relinquish primary management and administrative control of the subscribed software to Company. However, Client may elect to self-provision and self-manage some or all of the following elements:

- VMware Horizon (includes View Manager, View Composer and Persona Management)
- VMware ThinApp Client
- VMware ThinApp Packager
- VMware Workstation
- VMware vCenter Server Desktop
- VMware vSphere Enterprise Plus for Desktop

601722 HPE Data Protector Backup System Administration

Company's Responsibilities and Included Features

Company will provide support for a Client provided HPE Data Protector based backup solution ("Backup System"). The Backup System is comprised of a combination of supporting infrastructure (hardware) and HPE Data Protector backup software. Company will provide the following support:

Backup System Administration

- Configuration of backup policies
- Monitoring and reporting of backup status
- Re-submission of failed backup jobs as deemed appropriate by Company
- Hardware maintenance management
  - Manage hardware replacement with hardware vendor
  - Apply hardware BIOS updates as necessary
- System administration of the backup console and/or backup server(s) operating systems including:
  - Periodic review of backup software and console server operating system updates
  - Change notice submission, approval and application of point release system updates
  - Next version upgrade analysis and recommendations
- Major release version upgrades are not included within the scope of this support and will be scheduled as an independent project billed to Client on a time and materials basis as agreed upon by the Parties

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Where necessary Company will engage and log service requests with the software vendor in regard to software issues
- Provide Client with updates
- Document user issues and system errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General

- Open any necessary ports and conduits between Backup System and Company s management system
- Provide Company with access, passwords, access codes or security devices as necessary to perform the Services
- Provide or purchase all necessary equipment, cabling, circuits, and other materials required for the Services, unless Company explicitly provides that such materials are included as part of the Services
- Assist with any Backup System hardware repair or replacement as needed, and provide escorted access to the Backup System s authorized service vendors

Backup Software Licensing

- Procure backup software (server and agent) licensing for current version on current operating system
- Provide software media for installation, maintenance and configuration of the application
- Procure current software support and maintenance where applicable

Backup Operation

- Define backup content
- Define frequency, schedule, location and retention of the backups for data that require long-term retention
- Conduct operating system administration of servers subject to backup
- Validate data restored
- Install and manage backup agents on servers subject to backup if local agents are required
- Install any associated software (agents) on servers or infrastructure to be backed up
- Archive media operations and media including:
    - Media handling
    - Off-site and or secondary storage

End User Support

- Support of non-expert application end users

601759 Application Deployment Script Support in Azure Virtual Machine Scale Set (VMSS) Environment

Company's Responsibilities and Included Features

This service is provided as an add on to ItemID 601485 Azure VM Scale Set Management One Region and defines support activities for the application deployment scripts used for the promotion of the application that is using Azure VM scale sets.

Company will do the following to support the application deployment scripts in an Azure Virtual Machine Scale Set (VMSS) environment:

Incident Triage and Troubleshooting

- Troubleshoot existing scripts
- Modify existing scripts to rectify failures where applicable

Script Change Documentation

- Update script documentation to record changes made during script support

Service Delivery

- Service requests are to be requested through the Company Help Desk
- Application deployment support is limited to the number of hours per month as contracted. Based upon a rolling three (3) month average of hours consumed. Bursts in monthly consumption may not exceed 200% of contracted monthly hours.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Communications

Facilitate and be present in all communications with 3rd party

Script Issue Notification

- Notify Company when script issues occur

New Script Release

- Changes beyond fixes are outside of the scope of this ItemID and will be provided on a separate time and materials project basis

601769 Citrix XenAPP Server Management

Company's Responsibilities and Included Features

Citrix System Administration

- Citrix services availability and reliability management Requires that Citrix is deployed in a high availability configuration
- Citrix configuration
- Citrix security configuration
- Application load balancing rule management
- Installation of printer drivers to support Citrix supported business class printers
- System administration support for Citrix infrastructure issues
- Provide Windows server administration as needed for the Citrix XenApp server
- Requires a separate Citrix core infrastructure virtual machine/s, (independent of the workload delivery XenApp server) that deliver one or more of the following Citrix services
    - Delivery controller
    - Store-front server
    - Delivery server

Citrix Server Monitoring

Monitoring and review of:

- Citrix service availability
- Citrix application delivery availability
- IWindows Server health

Citrix Patch Management

- Periodic review of critical patches
- Up to quarterly routine review same version patch analysis and application
- Application of updates and patches during approved maintenance windows

If Client does not provide Company with a maintenance window to apply upgrades and patches within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Citrix Delivered Application Software Management

Support of applications loaded on the Citrix servers (CDA) will be limited to:

- Applying patches to CDAs in collaboration with the CDA s system administrators

Appliance Incident Triage and Troubleshooting

- Triage of server incidents
- Troubleshoot and work to resolve server incidents
- Document server issues and errors

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Citrix Delivered Application Software Licensing

- Procurement of CDA software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Citrix Application Software Licensing

- Procurement of Citrix software and licensing for current version on current operating system, including any user or processor access licensing
- Procurement of current software support and maintenance where applicable

Application Support

Support in the following areas of the CDAs loaded onto Citrix:

- Functional support
- Configuration of the application from within the application
- Application issue triage and resolution
- Patch identification
- Application installation and upgrades are out of scope for this SOW, but may be provided by Company under a separate time-and-material statement of work

Image Maintenance and Management

- Provide maintenance and management of server deployment images

Windows Management of Citrix Core Infrastructure VMs

- Contract for Company provided Microsoft Windows Server Management for all Citrix core infrastructure VMs

Citrix Infrastructure Architecture

- Client to ensure that Citrix is deployed in a high availability configuration if Company provided Citrix services availability and reliability management is required
- Requires a separate Citrix core infrastructure virtual machine/s, (independent of the workload delivery XenApp server) that deliver one or more of the following Citrix services
    - Delivery controller

Store-front server
- Delivery server

601875 Nutanix File Analytics Management

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services.

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Nutanix Files: A software-defined scale-out file storage solution designed to address a wide range of use cases, including but not limited to, support for Linux and Windows home directories, user profiles and department shares.

Nutanix File Analytics (Analytics): File Analytics provides dashboards and tools for monitoring the activity and contents of a Nutanix Files file server. It provides statistics and trends, the ability to audit users and files, and customize anomaly monitoring options.

SMB: Server Message Block, is a network protocol used by Windows-based computers that allows systems within the same network to share files.

Company's Responsibilities and Included Features

Analytics Management provides management services for the Analytics application available to customers running either mixed use or dedicated purpose Nutanix Files Clusters. Analytics provides data and statistics on the operations and contents of a file server. Analytics is deployed as a separate Virtual Machine (VM) within the cluster serving Nutanix Files.

Analytics management is quantified as per Analytics VM that participates within the Cluster delivering Files services.

Analytics Administration

Company will support the administration of the base application and its health. Analytics is by design, an end-customer self-service platform. Base application administration is defined as:

- Analytics VM configuration and management
  - Adjustments to provisioned resources includes vCPUs, memory, and storage
  - Performance monitoring and alert management
  - Configuration of data protection if requested by Client
    - Management of snapshots and Client defined retention schedules
    - If applicable management of asynchronous replication, protection domains, and schedules
    - If applicable, recovery from snaps
- Analytics Application
  - Manage network services for Analytics incoming and outgoing ports
  - Manage Analytics user role creation and role-based access level permissions
  - Manage data retention period per Client s policy. The data retention period is the length of time analytics retains audit events.
  - Manage Analytics authentication credentials
- Configuration management of SMTP services
  - Provide general Analytics usage guidelines and overview of the platform if requested by Client

Analytics and Troubleshooting

- Triage of Analytics incidents
- Troubleshooting of Analytics incidents

Document Analytics issues and errors

Analytics Patching, Updates and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the Analytics (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable timeframe based on the severity of the update, upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updating and upgrades are up to date. If patching, updating or upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time patching, updating or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for updates, upgrades and/or patches.

Co-administration

Company is providing managed Services on a virtualization platform with an end-user experience with the following self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
  - Interacting with the File Analytics dashboard
  - File Server alerts and notifications
  - File Server events

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Analytics Operations

In general, Analytics is self-service administration portal allowing Client to perform inquires against their Nutanix Files service, review system telemetry, and receive alerts based upon Client configured parameters. Operation of the platform is inclusive of but not limited to:

- Interact with Analytics dashboard
- Manage deleted share/export audits
- Manage File categories
- Configuration of anomaly detection
  - Definition of anomaly rules
  - Configure anomaly email recipients
- Operate audit trails feature

        - Select filter operations
    - Perform ad hoc file system scans
    - Define blacklisting rules

File Analytics Requirements

- Provide virtualizing resources to meet or exceed the Nutanix File Analytics specifications.
    - Minimum virtualized resources necessary to run the File Analytics VM:
        - 4 vCPU
        - 24 GB memory
        - 2 TB thin provisioned storage

Hardware and Software Licensing and Maintenance Coverage

- Procure Files software licensing, also available from Company under a separate ItemID.
- Procure all application licensing including but not limited to the Cluster OS, hypervisor and VM operating systems
- Procure and maintain hardware and software maintenance for the duration of the SOW
- Provide contract numbers and phone numbers for applicable hardware and software maintenance service providers
- Ensure that Company is an authorized caller to maintenance service providers

601957 Third Party Application Support

Company's Responsibilities and Included Features

General

Company shall provide administration of the application identified in this SOW/Change Order s Pricing Lines:

Additional details section as follows:

Administration and support is provided by USA resident resources and non-USA resident resources (onshore, offshore)

Application User Administration

Management of user identities within the application includes:

- User ID adds, changes, deletes
- Security group/role maintenance as applicable to the application as defined by the Client

Monitoring

- Monitor OS level services up-down status
- Monitor URL up-down status

Incident Triage and Resolution

Company will triage and manage the troubleshooting process for technical system errors.

Company will research problems and issues utilizing:

- Company knowledge of known errors and their solution
- General operating system level troubleshooting
- Escalation to software provider

Company will work to resolve system incidents through:

- Application of Company known solutions
- Application of software vendor provided solutions
- Resolution of application incidents can be dependent on software vendor response
- Engagement of software providers Help Desk support

- Documentation of application issues and system errors

Patching and Upgrades

Company shall provide patch application where patches for the application are within the following criteria:

- On demand, for up to four patch applications per year. Additional patching can be provided on a project, time and material basis
- Break-Fix/One-off/Hot-fix patches - Patch to address a specific failure to standard functionality (not a major of minor version change)

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Application Configuration

- Functional and technical application configuration

Database Administration

- Management of database if applicable

End-User Support and Management

- Support of end-users
- Application functional support
- Content or data related support or management
- End-user client software support

Development Support

Provide application development resources to develop new or modify existing configurations, extensions, modifications, localizations and integrations, including:

- Develop technical specification based upon functional requirements
- Develop or modify application objects/scripts
- Develop or modify reports
- Conduct unit and integration testing
- Document customizations

Application Software Licensing

- Procurement of application software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable

Performance Tuning

- Provide application performance tuning

Deployment, Redeployments and Environment Cloning

- Deployment or redeployment of applications
- Cloning to non-production environments. (Company can provide on a separately contracted project)

Patching

- Notify Company of the need for a patch
- User acceptance testing

Upgrades

- Any Major or Point release version upgrades. (Company can provide on a separately contracted project)

602085 File Transfer Services (FTP) Application Administration - GoAnywhere

Company's Responsibilities and Included Features

Company will provide systems administration for GoAnywhere Managed File Transfer software (MFT) as described herein.

MFT Application Administration

- MFT service availability monitoring
- Stop and restart services on Client request
- Provide logs to Client or GoAnywhere as necessary for troubleshooting

Incident Triage and Troubleshooting

Company will triage and manage the troubleshooting process for technical system errors. Company will research problems and issues reported by Client or Company monitoring system utilizing:

- Company knowledge of known errors and their solution
- General operating system level troubleshooting
- Working with GoAnywhere and Client to triage and troubleshoot issues

Resolution of system incidents:

- Application of Company known solutions
- Application of GoAnywhere provided solutions

Engagement of GoAnywhere s Help Desk support
Document user issues and system errors

Patching and Upgrades

Standard Patch Maintenance

Company shall provide patch application where patches for the application are within the following criteria:

- One-off patches - Patch to address a specific failure to standard functionality (i.e. Break-Fix)
- Any single or group of patches (Service Pack) required to solve a single issue or required by software vendor
- The patching activity is not associated with an application version upgrade

Major or Point Release Upgrades

Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties in an Executed Order.

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 8 am to 5 pm technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and a single point of contact for escalating incidents to Company. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating System Administration

- Requires Company contracted Operating System (OS) administration of the server on which the application is installed.

Application Configuration, End User Support and Management

- Support of non-Expert Users
- Application functional support
- Configuration of application
- Content or data related support or management
- End user client-side software support

Application Software Licensing and Vendor Management

- Procurement of application software and licensing for current version of MFT software on current operating system, including user and/or processor access licensing
- Providing software media for installation, maintenance and configuration of the GoAnywhere application
- Procurement of current software support and maintenance where applicable
- Client to be the Company s escalation point for contact to the vendor
- Client to authorize Company as a GoAnywhere vendor contact
- Client to provide MFT patches from GoAnywhere and notification to Company when a patch is to be applied

602566 Citrix Cloud on XenApp Administration

Company's Responsibilities and Included Features

General

Company will provide administration of a Citrix XenApp based VDI environment using Citrix Cloud for orchestration as described herein

Citrix System Administration

- XenApp application delivery services management
- Web interface management
- Shared published desktop management
- User rights administration
- Policy management
- Citrix services availability and reliability management Requires that Citrix is deployed in a high availability configuration
- Citrix configuration
- Citrix security configuration
- Application load balancing rule management
- Installation of printer drivers to support Citrix supported business-class printers
- Provide Windows server administration as needed for the Citrix XenApp server
- Citrix XenApp patching

Citrix Receiver client configuration documentation
- Manage antivirus system updates
- Streaming application support via XenApp and/or App-V
- Major corruption recovery to image level Operating System only

Citrix Cloud and XenApp Triage and Troubleshooting

- Triage of Citrix Cloud and XenApp system incidents
- Troubleshoot and work to resolve Citrix Cloud and XenApp system incidents
- Escalation of system issues to Citrix where necessary
- Document Citrix Cloud and XenApp system issues and errors

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4, and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with an in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide support for client hardware (i.e. physical desktops, thin clients, mobile devices, printers, peripherals) and their operating systems
- Provide Client hardware that has been verified as 'Citrix Ready' can be found at http://citrix.com/ready
- Provide supported desktop Operating System licenses
- Client application upgrades/updates
- Client application patching for other than Operating System security
- Multi-factor authentication
- WAN services
- Local network environment (i.e. network hardware, cabling, etc.)
- VPN client support when installed
- Geographic (DR) redundancy
- Recovery beyond Operating System image
- Backup of any data. Can be provided under a separately contracted ItemID
- End user support

Citrix Delivered Application (CDA) Software and OS Licensing

- Procurement of CDA software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the application
- Procurement of current software support and maintenance where applicable
- Provide supported desktop Operating System licenses
- Provide Client Access Licenses (CALs) where necessary

Citrix Software Licensing

- Procurement of Citrix software and licensing for current version on current operating system with Citrix Cloud, including any user or processor access licensing

Client Application Support

Support in the following areas of the CDAs loaded onto Citrix XenApp:

- Functional support
- Configuration of the application from within the application
- Application issue triage and resolution
- Patch identification
- Application installation and upgrades are out of scope for this SOW but may be provided by Company under a separate time-and-material statement of work

Image Maintenance and Management

- Client application packaging. Can be provided under a separately contracted ItemID
- Desktop Image creation, deployment, and support. Can be provided under a separately contracted ItemID

Citrix Infrastructure Architecture

- Client to ensure that Citrix is deployed in a high availability configuration if Company provided Citrix services availability and reliability management is required
- Requires a separate Citrix core infrastructure virtual machine/s, (independent of the workload delivery XenApp server) that delivers Citrix Cloud Connector or the Citrix appliances necessary for the environment Citrix core infrastructure

Windows Management of Citrix Core Infrastructure VMs

- Contract for Company provided Microsoft Windows Server Management for all Citrix core infrastructure VMs

User Support and Device Administration

- End-use device management
- Printer device management
- End-user support

603271 ReliaCloud EDGE Service Catalog Service - Level 1

Definitions

Application VM: A virtual machine (VM) or appliance that supports that operation and function of a specific application or defined set of applications. Application VMs are launched from Nutanix Blueprints

Categories: A logical grouping of Application VMs using metadata tags for purpose such as, but not limited to; cost allocation, reporting, compliance, and security. A Category is a combination of a key and values.

Endpoint: A VM or IP address. Endpoints are commonly described as a Microsoft Windows based VM, a Linux based VM, or an HTTP service endpoint.

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Nutanix Blueprint: Blueprints are templates that describe all the steps that are required to provision, configure, and execute tasks on the services and applications that you create.

Nutanix Calm: Calm Cloud Application Life Cycle Manager, software running within the Cluster or in a Nutanix Software a as Service Cloud. Calm allows you to select, provision, and manage your business applications across your infrastructure for both the private and public clouds. Calm provides application automation, lifecycle management, monitoring, and remediation to manage your infrastructure.

Project: Inside of Nutanix Calm, a Project is a set of Active Directory users with a common set of requirements or a common structure and function, such as a team of engineers collaborating on an engineering project.

Runbook: A collection of tasks that are run sequentially at different endpoints.

Showback: A feature which displays a derived and estimated cost of the service consumed.

Company's Responsibilities and Included Features

ReliaCloud EDGE Service Catalog Service Level 1 (SCS-1) is a combination of software licensing and managed services around maintaining a customized IT service catalog of standardized blueprints. SCS-1 leverages Nutanix Calm as the platform software to facilitate the application life cycle management.

SCS-1 is designed to be a Client (end user) driven platform to simplify, standardize, and expedite the deployment of Client applications into their Cloud environments through self-service. Calm supports several cloud environments including but not limited to ReliaCloud, Microsoft Azure and AWS.

Calm Features:

Company will provide an EDGE Node that meets or exceeds the following physical specifications:

- Self-service user interface for provisioning and managing Application VMs
    - Calm provides an alternative interface for VM administration from the administration interfaces of public clouds such as Microsoft Azure and AWS.
    - Application VM actions include but are not limited to create, start, stop, restart, delete, update (edit), install Nutanix guest tools.
    - Application VM metrics and Audit trails
- Role-based Access control using Nutanix Projects
- Multi-Cloud orchestration through a single common interface
- End-to-end activity logging and traceability
- Nutanix Marketplace, an ordering portal for launching blueprints and runbooks
- Cost governance with Showback awareness
- Application Development Platform with Calm DSL Infrastructure-as-CODE.

Product Consumption:

SCS-1 Is consumed based upon the contracted number of Application VMs that are managed through Nutanix Calm. Client may choose to remove Application VMs from Calm management, once launched. Application VMs under Calm management may be interchanged (swapped) throughout the course of the month, up to the contracted amount. The total number of contracted Application VMs can be added or removed via a service order.

Calm Administration:

- Calm administration for the following:
    - Settings
    - Licensing
    - Calm software upgrades
    - Showback enablement /configuration
    - Policy engine enablement /disablement and configuration
        - Approval policy creation/modifications are not covered under this scope and available as a scoped Statement of Work on a time and materials basis.
- Ad hoc Calm data backups
- VPC tunnel configuration between Prism Central instances to support multi-Prism Central configuration.
- Provider account configuration
- Project creation and configuration
- Marketplace
    - Enablement
    - Add or remove (publish/unpublish) and delete blueprints. SCS-1 doesn t include blueprint creation. Blueprint creation and modifications are available as a scoped Statement of work on a time and materials basis.
    - SCS-1 contains a public library of blueprints that can be enabled upon request. The public library is not

maintained by Company, and may not meet our standards for service management, nor will they support integrations for Company management.

- Brown Field Applications. Brown field applications are Application VMs that were not initially created from within Calm.
  - Upon Client request Company will execute the Brown Field Application creation feature for Client identified Application VMs. Company and Client will work to define parameters such as but not limited to:
    - Application name
    - Description
    - Project association
    - Credentials
    - Launch brown field applications

Blueprint and Script Administration:

Blueprint and script administration is only provided for Blueprints and scrips that have been created, tested, and validated by Company Professional Service and or Managed services, or a Company supported partner/vendor.

Administration is limited to troubleshooting of failed processes and actions within the Blueprint or script. Troubleshooting flow stops at the demarcation of Company provided managed services.

Example, if an Endpoint is not under company management, and an action, process, or integration fails. Or if a managed Endpoint fails due to a problem with an integration that is not under Company management, such as but not limited to a Client managed ticketing system, ERP, database

Expert User Technical Support:

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements:

- Contract with Company for a ReliaCloud EDGE cluster(s)
- Contract for third party Cloud services such as Microsoft Azure or AWS if applicable
- Own and manage guest VM applications and operating systems support

Third Party Utilities and Applications:

- Manage third-party AHV enhancement tools, utilities and applications

Blueprints, Scripts, Runbooks :

- Planning, development and creation
- Troubleshooting, triage and resolution
- Contract for third party development or design services
- Endpoint integration to Client services
- Management of Client created libraries in Calm
- Define, create, and manage and approval policies
- Define and create Categories

Acknowledgment and EULA:

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix Calm is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

603830 Citrix DaaS MCS System Administration - Base

Company's Responsibilities and Included Features

General

Company will provide administration of the Client's Citrix Desktop-as-a-Service (DaaS) system as described herein.

This service has a base fee that will be billed under this ItemID and additional named user volume-based fees priced and billed under additional ItemIDs

The named user fees is a metered service and will be billed based upon the number of named users who launched a virtual desktop during the billing period.

System Administration

System administration of the Citrix DaaS system, includes:

- Citrix license administration
- Monitor license usage
- Cloud connector administration
  - Monitoring
- User profile administration (excluding third party enterprise profile solutions)
  - Profile resets
  - Custom tuning of start menu for application presentation
- Workspace administration or on-prem storefront
- Alert monitoring
- Infrastructure capacity administration
- Citrix application performance optimization tuning utilizing Citrix HDX policies
- Citrix network performance policy optimization utilizing Citrix HDX policies
- Monitoring utilization (Compute, storage, network bandwidth)
- Reporting on utilization
- Infrastructure performance monitoring
- Optimization of settings
- Published applications and desktop administration
- Identity and access management of:
  - User authentication methods
    - Azure Active Directory
    - Active Directory
    - Citrix Gateway
  - User authorization rules
- User identity if using Basic identity management
- Domain joined accounts
- General configuration options administration
- Citrix policies administration
  - Time limits
  - Features On/Off
- Maintain customer/organization Features
- Storefront branding colors and logo only

Citrix Incident Triage and Troubleshooting

- Triage of Citrix incidents
- Troubleshoot and work to resolve Citrix incidents
- Document system issues and errors
- Support escalation to Citrix for system errors/bugs

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, or Client help desk available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Active Directory

- Provide Company administrative access to Citrix-related Organizational Units (OU) in Active Directory and Group Policy

Licensing

- Provide Citrix licensing or subscribe to Company provided Citrix licensing
- Provide Nvidia licensing or subscribe to Company provided Nvidia vGPU licensing if GPU are used
- Provide desktop OS licensing
- Provide SSL Certificates

Network Connectivity

- Provide necessary network connectivity (bandwidth and latency) between the end user device and the DaaS platform

Image Management

- Maintaining the gold image which typically includes:
    - Windows Operating system patching
    - Applying antivirus updates
    - Applying application patches
    - Adding new applications
    - Removing applications
    - Publishing image to users
    - Troubleshooting and resolving image issues
- This may be provided under a separate ItemID

Antivirus Management

- Providing antivirus protection
- Managing antivirus system and updates

Persistent Desktop Administration

- Provide patching, backup, and administration of persistent desktops. This may be provided under a separate ItemIDs

End User and End User Device support

- Provide end user support
- Provide end application support for all applications in the image
- Provide end user device and network support, maintenance, configuration

603831 Citrix DaaS System Administration - Named User up to 200 users

Company's Responsibilities and Included Features

General

Company will provide Citrix DaaS system administration for up to 200 named users as described in ItemID 603830 Citrix System Administration - Base.

The named user fees are a metered service and will be billed based upon the number of named users who launched a virtual desktop during the billing period.

ItemID 603830 Citrix System Administration - Base. is a pre-requisite for this ItemID

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

The scope of Client responsibilities is as per ItemID 603830 Citrix System Administration - Base.

603832 Citrix DaaS System Administration - Named User Over 200 up to 500 users

Company's Responsibilities and Included Features

General

Company will provide Citrix DaaS system administration for users in excess of 200 named users up to 500 named users as described in ItemID 603830 Citrix System Administration - Base.

The named user fees are a metered service and will be billed based upon the number of named users who launched a virtual desktop during the billing period.

ItemID 603830 Citrix System Administration - Base. is a pre-requisite for this ItemID

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

The scope of Client responsibilities is as per ItemID 603830 Citrix System Administration - Base.

603833 Citrix DaaS System Administration - Named User over 500 up to 1000 users

Company's Responsibilities and Included Features

General

Company will provide Citrix DaaS system administration for users in excess of 500 named users up to 1000 named users as described in ItemID 603830 Citrix System Administration - Base.

The named user fees are a metered service and will be billed based upon the number of named users who launched a virtual desktop during the billing period.

ItemID 603830 Citrix System Administration - Base. is a pre-requisite for this ItemID

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

The scope of Client responsibilities is as per ItemID 603830 Citrix System Administration - Base.

603834 Citrix DaaS System Administration - Named User 1000 up to 2000 users

Company's Responsibilities and Included Features

General

Company will provide Citrix DaaS system administration for users in excess of 1000 named users up to 2000 named users as described in ItemID 603830 Citrix System Administration - Base.

The named user fees are a metered service and will be billed based upon the number of named users who launched a virtual desktop during the billing period.

ItemID 603830 Citrix System Administration - Base. is a pre-requisite for this ItemID

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

The scope of Client responsibilities is as per ItemID 603830 Citrix System Administration - Base.

603835 Citrix DaaS System Administration - Named User over 2000 users

Company's Responsibilities and Included Features

General

Company will provide Citrix DaaS system administration for users in excess of 2000 named users as described in ItemID 603830 Citrix System Administration - Base.

The named user fees are a metered service and will be billed based upon the number of named users who launched a virtual desktop during the billing period.

ItemID 603830 Citrix System Administration - Base. is a pre-requisite for this ItemID

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

The scope of Client responsibilities is as per ItemID 603830 Citrix System Administration - Base.

603836 Citrix Image Maintenance and Administration

Company's Responsibilities and Included Features

General

Company will provide systems maintenance and administration of a single Microsoft Windows desktop image as described herein. This service requires that the Client is contracted for Company provided Citrix DaaS System Administration.

Gold Image Maintenance and Administration

Patching and troubleshooting of applications within the image is limited to any 5 of the Standard VDI Applications as listed on https://www.OneNeck.com/StandardVDI-Applications . Company may elect to add or remove applications to or from this list at any time. Additional Standard or non-standard VDI Applications may be contracted for under separate ItemIDs

Gold image maintenance and administration includes:

- Consultation with Client to review the specific change requirements of the image to be updated or modified as identified by Client and or Company
- Patching of a currently supported Microsoft desktop OS and/or driver updates as requested by the Client
- Patching of a Standard VDI Applications as requested by the Client
- Removal of any installed Standard VDI applications
- Installation of Standard VDI Applications post initial development of image
- Backup and storage of non-persistent desktop images up to three previous versions
- Backup and storage of a single persistent desktop image

Publication of updated images to end user test group
- Publication of Client approved images to production users
- Company will only manage applications on the image that have been setup or configured based upon application vendor s best practices
- Failover of users to an alternate site if Client has contracted for alternate locations for DaaS workloads in the event of a failure of the primary workload location
- Upgrades to a new major version of the OS or embedded OS application are outside of the scope of this ItemID and may be provided on a separate time and materials project basis
- Upgrades to a new major version of applications are outside of the scope of this ItemID and may be provided on a separate time and materials project basis
- Management of the gold image maintenance cycle as described below

Gold Image Maintenance Cycle

Maintenance of the Client s image is conducted typically over a 4-week maintenance cycle, but no shorter that a 4-week cycle. The 4-week duration may be lengthened by Client after consultation with Company. Each image is thus limited to one standard production update and publication of the image per maintenance cycle. Each Gold Image will have two Citrix Accounts. One Citrix Account will be for production usage and the second Citrix Account will be for image development and User Acceptance Testing (UAT).

The maintenance cycle is conducted as follows:

Week 1:

1. Patching and updating gold image in UAT Citrix Account which includes:
    - Windows Operating system patching
    - Applying antivirus application updates excludes AV definitions/heuristics
    - Applying Standard VDI Application patches
    - Adding new Standard VDI Applications
    - Removing Standard VDI Applications
    - Updating/changing image configuration
2. Publishing UAT image to UAT group of users
3. Notification to Client that a new image is to be tested in UAT Account

Week 2:

1. Client lead user acceptance testing is conducted
2. Notification by Client to Company of issues with the UAT image
3. Updates are made to the gold image as identified by the UAT group
4. Republishing of UAT image as necessary
5. Client provides acceptance that image is ready to be published to production users

Week 3:

1. UAT image is copied to production Account
2. Publishing of production image
3. Notification to Client that the new image is now in production

Week 4:

1. Client to notify Company of any issues with the new image that was not identified during prior week s testing
2. Rectification of production image issues and republishing
3. Client identifies and notifies Company of updates and changes needed to be applied in the next maintenance cycle.
4. Any issues that are found once the image has been published to production that the Client requires to be resolved before the next maintenance cycle may be addressed on a separate time and materials project basis

Citrix Image Incident Triage and Troubleshooting

- Triage of Citrix image incidents
- Troubleshoot and work to resolve Citrix image incidents
- Triage and troubleshooting of non-standard VDI applications are outside of the scope of this ItemID and may be contracted for under a separate ItemID
- Troubleshooting of application or cross-application dependencies when patching applications will be limited to 1 hour per application per patch cycle. Any further Company effort to troubleshoot when patching applications may be billed to Client by Company on an hourly basis.
- Document system issues and errors
- Support escalation to Citrix for system errors/bugs
- Support escalation to Standard VDI Application vendor

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, or Client help desk available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Active Directory

- Provide Company administrative access to Citrix-related Organizational Units (OU) in Active Directory and Group Policy

Licensing

- Provide Desktop OS licensing
- Provide licensing for all applications used in the image as applicable

User Acceptance Testing

- Provide timely testing of the images during the second week of the Gold Image Maintenance Cycle
- Provide rigorous testing of the UAT image to ensure minimal subsequent issues once the image is published to production
- Clear and timely notification to Company of issues found with the UAT image

Application Troubleshooting and Application Vendor Support

- Work collaboratively with Company to troubleshoot application issues
- Provide Company with representative user account/s to enable Company testing of the image
- Provide access to application vendor support for troubleshooting of patching issues

Identification and Notification of Changes Needed

- Identify updates or changes needed to image
- Notify Company of updates or changes needed to image, prior to start of new Gold Image Maintenance Cycle

Antivirus Management

- Providing antivirus protection
- Managing antivirus system and updates

Administration of Persistent Desktops

- Antivirus administration
- Patching

603837 Citrix Image Maintenance and Administration - Additional Standard Applications

Company's Responsibilities and Included Features

General

Company will provide Citrix Image Maintenance and Administration for additional Standard VDI Applications over and above the 5 Standard VDI Applications included in ItemID 603836 Citrix Image Maintenance and Administration. The specifications of management for the additional Standard VDI Applications are the same as described in ItemID 603836 Citrix Image Maintenance and Administration.

ItemID 603836 Citrix Image Maintenance and Administration is a pre-requisite for this ItemID

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

The scope of Client responsibilities for the additional Standard VDI Applications is as per ItemID 603836 Citrix Image Maintenance and Administration Client responsibilities.

603838 Citrix Image Maintenance and Administration - Non-Standard Applications

Company's Responsibilities and Included Features

General

Company will provide Citrix Image Maintenance and Administration for Non-standard VDI applications. The scope of management for the Non-Standard VDI Applications is as described herein.

Non-standards VDI applications are defined as applications not contained in the list of Standard VDI Applications as published on https://OneNeck.com/StandardVDI-Applications .

ItemID 603836 Citrix Image Maintenance and Administration is a pre-requisite for this ItemID and provides the framework under which the non-standards VDI applications will be managed.

Additionally, non-standard VDI applications will also be managed as described herein:

Gold Image Maintenance and Administration

Gold image maintenance and administration of non-standard applications includes:

- Consultation with Client to review the specific change requirements of the image to be updated or modified as identified by Client and or Company
- Patching of a non-standard VDI applications as requested by the Client
- Removal of any installed non-standard VDI applications
- Company will only manage applications on the image that have been setup or configured based upon application vendor s best practices
- Installation of non-standard VDI applications is outside of the scope of this ItemID and may be provided on a separate time and materials project basis
- Upgrades to a new major version of applications are outside of the scope of this ItemID and may be provided on a separate time and materials project basis

Citrix Image Incident Triage and Troubleshooting for Non-Standard Applications

- Troubleshooting of application or cross-application dependencies when patching non-standard applications will be limited to 2 hours per application per patch cycle. Any further Company effort to troubleshoot when patching applications may be billed to Client by Company on an hourly basis.
- Document system issues and errors

- Support escalation to Citrix for system errors/bugs
- Support escalation to non-standard VDI application vendor or Client

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

The scope of Client responsibilities for the non-standard VDI applications is as per ItemID 603836 Citrix Image Maintenance and Administration Client responsibilities.

604402 EDI Application Support

Company's Responsibilities and Included Features

TrustedLink Enterprise EDI Support*

EDI support provides qualified resources to provide supplemental support for a OpenText TrustedLink Enterprise EDI (TLE) application. This support can include any of the following areas within TLE:

- Monitor delinquent functional acknowledgement report and research and resolve any discrepancies received
- Check all email received from EDI translator throughout the day for errors in translation or communication
- Execute monthly archiving of inbound and outbound data (i.e X12 and/or EDIFACT)
- Advise Client EDI Manager of issues
- Update ticket as appropriate based on solution or failures or projects
- Mapping changes will require Client approval
- Resend EDI documents as appropriate
- Acknowledge any tickets opened by Company monitoring tools
- Ensure successful translation of inbound/outbound EDI documents per trading partner requirements
- Validate all data inbound/outbound has been received/sent successfully via VAN, AS2 or FTP communications
- General EDI application issue analysis and troubleshooting
- Assist client in diagnosing or analyzing functional issues as they pertain to EDI

EDI support is provided during the business hours of 6:00 AM PDT to 3:00 PM PDT, Monday through Friday, excluding normal Client holidays.

* EDI Support is limited to number of hours per month as contracted

610416 CISE Virtual Machine Management

Company's Responsibilities and Included Features

Management Details

- Managed Services - ISE Virtual Machine shall be a Resource Category. One (1) Resource Unit for this Resource Category shall be equal to one (1) virtual Cisco Identity Services Engine appliance providing secure access and authentication to users (i) that is dedicated to the City, and (ii) for which the City has requested and approved Supplier s provision of Services.
- The management of all Cisco ISE Virtual Machines shall by extension mean that OneNeck fully manages the Cisco ISE ("Identity Services Engine") application for Client.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Access

- Facilitate access into the environment for service delivery.

Category: Managed Collaboration

103013 Xmedius Fax Server Management

Company's Responsibilities and Included Features

Configuration

- Troubleshoot incoming/outgoing fax failures. (Failure must be identified by local resource as not being due to user error or circuit unavailability/congestion)
- Troubleshoot system-related issues impacting fax server operation (fax manager, fax drivers and rasterization services)
- Troubleshoot fax client issues
- Troubleshoot client issues
- Troubleshoot fax solution for minor configuration-related tasks.

Minor changes are defined as those that take two hours or less to plan, implement and test, collectively. Major changes will be billed on a time and materials basis in addition to the monthly service fee for Management. Additional configuration and administration changes are also available on a time and materials basis.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Perform additional disaster recovery tasks
- Troubleshoot end-user desktop issues
- Support third-party systems or software (unless managed by Company)
- Manage and verify antivirus signature file updates (unless managed by Company)
- End user training
- Make major fax server configuration changes (available as a Project)
- Perform minor/major version upgrades (available as a Project)

Category: Managed Databases

100081 Microsoft SQL Analysis Services (SSAS) Management

Company's Responsibilities and Included Features

Analysis Services System Administration Manage the following areas within the Microsoft SQL Server Analysis Services:

- Object deployment
- Object impact analysis, starting and reprocessing
- Batch processing management
- SQL Integration Services (SSIS) application management as related to the usage of SSIS for Dynamics AX reporting through SQL Server Reporting Services
- Monitoring Analysis Services availability and performance object change management:
- Deployment and migration of objects through development, test, QA environments (as applicable) through to production
- Change control

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Analysis Services Development and Content Management

- Development and maintenance of solutions, projects, scripts and objects
- Content management
- Application and database usability
- Diagnosis and resolution of processing failures related to content or solutions, projects, scripts and objects Database Software Licensing
- Procurement of database software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the database
- Procurement of current software maintenance where applicable End User Support and Management
- Support of non-super users
- Application functional support
- Content or data related support
- End user client software support Third Party Application Dependency Management
- Management of third party application interface to the database

100082 Microsoft SQL Integration Service Management (SSIS)

Company's Responsibilities and Included Features

SQL SSIS Management Manage the following areas within the Microsoft SQL Services Integration Services:

- Integration Windows Service
- Integration Services Log Files
- SQL Integration Services (SSIS) application Monitoring Integration Server Availability and Performance
- Custom object change management:
- Migration of customizations through development, test, QA environments (as applicable) through to production Database Software Patch Management
- Monthly reviews of critical patches
- Up to quarterly routine review same-version patch analysis and application
- Periodic next version upgrade analysis and recommendations
- Application of updates and patches during approved maintenance windows Major or Point Release Upgrades
- Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

SQL SSIS Management

- Client Database Software Licensing
- Procurement of database software and licensing for current version on current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the database
- Procurement of current software maintenance where applicable End User Support and Management
- Support of non-super users
- Application functional support
- Content or data related support

- End user client software support Database Schema and Content Management
- Development and/or customization of database schema
- Content management Integration Services Development
- Development and maintenance of SIS packages and the integration with items outside of SQL (i.e. applications, etc.)
- Diagnosis and resolution of processing failures related to items outside of SQL (i.e. applications, etc.) Third Party Application Dependency/Relationship Management
- Management of third party application interface to the database

100088 Microsoft SQL Reporting Service Management (SSRS)

Company's Responsibilities and Included Features

Reporting Services System Administration Manage the following areas within the Microsoft SQL Services Reporting Services:

- Report Server Web Service
- Reporting Windows Service
- Reporting Services Log Files
- SQL Integration Services (SSIS) application management as related to the usage of SSIS for Dynamics AX reporting through SQL Server Reporting Services. Monitoring Report Server Availability and Performance Custom object change management:
    - Migration of customizations through development, test, QA environments (as applicable) through to production
    - Change control 24x7x365 Help desk support

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Database Schema and Content Management

- Development and/or customization of database schema
- Content management Database Software Licensing
- Procurement of database software and licensing for current version on current operating system including
    - Any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the database
- Procurement of current software maintenance where applicable End User Support and Management
- Support of non-super users
- Application functional support
- Content or data related support
- End user client software support
- Reporting Services Development
- Development and maintenance of reports, scripts and objects
- Diagnosis and resolution of processing failures related to content or reports, scripts and objects
- Third Party Application Dependency Management
- Management of third party application interface to the database

103041 Database Monitoring Only (per instance)

Company's Responsibilities and Included Features

- Deploy and configure monitoring of database application using Company standard template
- Supported technologies:

All database applications supported under Company managed services

- Configure monitoring of:
  - Database specific services

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Resolve issues identified by Company monitoring
- Provide appropriate escalation path for alerts
- Work with Company to adjust and tune alerting thresholds
- Provide appropriate credentials to enable monitoring
- Configure network and devices to meet monitoring requirements

600030 Microsoft SQL database refresh

Company's Responsibilities and Included Features

Database Refresh

A database refresh is defined as the process of taking a copy of a single database (usually production) and restoring it to a target database.

The Company process involves using the latest or a prior copy of the database hot backup that has already occurred, to restore to the target environment.

Company will execute the cloning process on request or on predefined schedules, which can include the following:

- Running post-restore database scripts
- Notification of completion of refresh

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Database Refresh Request

- Database refresh must be scheduled at least 3 business days in advance.
- Database refresh request must originate from a user approved to request a refresh to the target database.
- Users must log out of the target database prior to scheduled start of refresh.

600032 Oracle database support

Company's Responsibilities and Included Features

Oracle Database Support*

Oracle database support provides qualified resources to manage Oracle databases within the monthly bucket of hours as contracted.

This includes the following areas within the Oracle database:

Setup

- Installation, setup and configuration of new database instances
- Setup Oracle RAC

Management

- Transaction log maintenance
- Memory utilization/configuration
- Transaction log files
- Table and index storage parameters
- Table and index fragmentation

  Database storage parameters

- Instance and database configuration options
- Connectivity
- Table statistics
- Database issues such as table locks/record contention
- Database cluster management
- Database backup administration
- Database security administration

Review and/or make recommendations within the following areas:

- Database software configuration
- Physical and logical disk layout
- Backup and disaster recovery design strategies based on business needs
- Repository database creation for reporting or other peripheral tools creation
- Redistribution of data files
- Schema changes

* Oracle Database Support is limited to number of hours per month as contracted.

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Engagement of software providers Help Desk support (requires Client to have a support contract with the software provider)
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues
- Provide client with updates

Document user issues and system errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Database Software Licensing

- Procurement of database software and licensing for current version on current operating system,
- including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the database
- Procurement of current software maintenance where applicable

System Administration

System administration of the server operating system including:

- Operating system configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks

600117 Oracle database administration - Standard

Company's Responsibilities and Included Features

Oracle Database Administration

Manage and tune the following areas within the database:

- Redo log maintenance
- Memory utilization/configuration
- Table and index storage parameters
- Table and index fragmentation
- Instance and database configuration options
- Oracle Net configuration and maintenance
- Optimizer statistics (tables, indexes, histograms and system statistics
- Concurrency (table/row locks)
- RAC (if applicable)

Review and/or make recommendations within the following areas:

- Database software configuration
- Physical and logical disk layout
- Database instance creation
- New database provisioning
- Backup and disaster recovery design strategies based on business needs
- Repository database creation for reporting or other peripheral tools creation
- Redistribution of data files
- Schema changes
- Query/explain plan analysis

* Implementation of recommendations will be handled on a per project time and material basis.

Database Incident Triage and Troubleshooting

- Triage of database system incidents
- Troubleshooting of database system incidents
- Engagement of Oracle support
- Document user issues and database system errors

Database Monitoring

- Configuration of database monitoring thresholds and parameters
- Monitoring and reporting of key metrics including:
- Database availability
- Space usage
- Blocking locks
- Concurrent sessions
- Periodic capacity planning

Database Backup Management

- Configuration of database backup
- Monitoring of database backup status
- Rectification and resubmission of failed backup jobs as appropriate
- Adhoc backup or restore on request, limited to four per year
- Quarterly test restores

Database Software Patch Management

- Review of patches upon request or for specific bugs or issues
- Application of updates and patches during approved maintenance windows

Database Management Documentation

- Document applicable database administration procedures

Database Security Management

- User creation and security maintenance
- Database encryption and audit management where appropriate

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Database Software Licensing

- Procurement of database software and licensing for current version on current operating system,
- including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the database
- Procurement of current software maintenance where applicable

Third Party Application Dependency Management

- Management of third party application interface to the database

Database Schema and Content Management

- Development and/or customization of database schema
- Content management

Database Upgrades

- Major or point release upgrades - Any major or point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

600118 Oracle database administration - Complex

Company's Responsibilities and Included Features

Oracle Database Administration

Manage and tune the following areas within the database:

- Redo log maintenance

- Memory utilization/configuration
- Table and index storage parameters
- Table and index fragmentation
- Instance and database configuration options
- Oracle Net configuration and maintenance
- Optimizer statistics (tables, indexes, histograms and system statistics
- Concurrency (table/row locks)
- RAC (if applicable)

Review and/or make recommendations within the following areas:

- Database software configuration
- Physical and logical disk layout
- Database instance creation
- New database provisioning
- Backup and disaster recovery design strategies based on business needs
- Repository database creation for reporting or other peripheral tools creation
- Redistribution of data files
- Schema changes
- Query/explain plan analysis

* Implementation of recommendations will be handled on a per project time and material basis.

Database Incident Triage and Troubleshooting

- Triage of database system incidents
- Troubleshooting of database system incidents
- Engagement of Oracle support
- Document user issues and database system errors

Database Monitoring

- Configuration of database monitoring thresholds and parameters
- Monitoring and reporting of key metrics including:
- Database availability
- Space usage
- Blocking locks
- Concurrent sessions
- Periodic capacity planning

Database Backup Management

- Configuration of database backup
- Monitoring of database backup status
- Rectification and resubmission of failed backup jobs as appropriate
- Adhoc backup or restore on request, limited to four per year
- Quarterly test restores

Database Software Patch Management

- Review of patches upon request or for specific bugs or issues
- Application of updates and patches during approved maintenance windows

Database Management Documentation

- Document applicable database administration procedures

Database Security Management

- User creation and security maintenance
- Database encryption and audit management where appropriate

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Database Software Licensing

- Procurement of database software and licensing for current version on current operating system,
- including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the database
- Procurement of current software maintenance where applicable

Third Party Application Dependency Management

- Management of third party application interface to the database

Database Schema and Content Management

- Development and/or customization of database schema
- Content management

Database Upgrades

- Major or point release upgrades - Any major or point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed

upon by the Parties.

600141 Oracle database disaster recovery from backup

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of a database in a Recovery Site acting as a failover database.

Replication of the database binaries and non-database file systems from the primary server to the target DR server is to be provided through the use of server to server replication software or manual application of sofware changes, and requires an OS replication Service Item which will perform the replication or database software updates.

Recovery of the databases will be accomplished through the use of the periodic database backup produced as part of the source database management services.

Company shall develop and maintain Disaster Recovery Failover Procedures. These procedures will be available at the Recovery Site.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR database is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Database Software Patch Management

- Review of patches upon request or for specific bugs or issues
- Application of updates and patches during approved maintenance windows

Database Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of failover tests per year is referenced in Pricing Parameters.
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster occur during a test, the data will be as old as the data was when testing began.

Database Failover Services

- On declaration of a disaster, Company will perform the steps necessary to restart and validate the database on the target DR server and make it the primary database, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the primary server, database administration of the database will be as per the administrative, support, backup and monitoring services as defined for the primary database.

Database Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and

return service back to the Primary Site.

- The database administrator will assist the operating systems administrator reestablish database replication back to the target DR server.
- Database server Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Database Software Licensing

- Procurement of database software and licensing for current version on current operating system,
- including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the database
- Procurement of current software maintenance where applicable

OS Management or OS Level Replication Software, Infrastructure and Management

Management of the underlying operating system of the target DR server to maintain it to the same level as the primary database server is required.
This can be accomplished through manual management of the operating system or through OS based replication software.

600142 Microsoft SQL database disaster recovery from backup

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of a database in a Recovery Site acting as a failover database.
Replication of the database binaries and non-database file systems from the primary server to the target DR server is to be provided through the use of server to server replication software or manual application of sofware changes, and requires an OS replication Service Item which will perform the replication or database software updates.
Recovery of the databases will be accomplished through the use of the periodic database backup produced as part of the source database management services.
Company shall develop and maintain Disaster Recovery Failover Procedures. These procedures will be available at the Recovery Site.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time,

backwards from the point of disaster.

- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR database is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Database Software Patch Management

- Review of patches upon request or for specific bugs or issues
- Application of updates and patches during approved maintenance windows

Database Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of failover tests per year is referenced in Pricing Parameters.
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster occur during a test, the data will be as old as the data was when testing began.

Database Failover Services

- On declaration of a disaster, Company will perform the steps necessary to restart and validate the database on the target DR server and make it the primary database, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the primary server, database administration of the database will be as per the administrative, support, backup and monitoring services as defined for the primary database.

Database Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The database administrator will assist the operating systems administrator reestablish database replication back to the target DR server.
- Database server Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Database Software Licensing

- Procurement of database software and licensing for current version on current operating system,
- including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the database
- Procurement of current software maintenance where applicable

OS Management or OS Level Replication Software, Infrastructure and Management

Management of the underlying operating system of the target DR server to maintain it to the same level as the primary database server is required.
This can be accomplished through manual management of the operating system or through OS based replication software.

600143 Oracle database disaster recovery management via DataGuard

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of an Oracle Database in a Recovery Site acting as a failover database.
Replication of the database binaries and non-database file systems from the primary server to the target DR server is to be provided through the use of server to server replication software and requires an OS replication Service Item which will perform the replication.
Replication of the databases will be accomplished through the use of the native Oracle DataGuard replication services.
Company shall develop and maintain Disaster Recovery Failover Procedures. These procedures will be available at the Recovery Site.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR database is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Database Software Patch Management

- Review of patches upon request or for specific bugs or issues
- Application of updates and patches during approved maintenance windows

DataGuard Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents

- Troubleshooting of replication incidents.

Database Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of failover tests per year is referenced in Pricing Parameters.
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster occur during a test, the data will be as old as the data was when testing began.

Database Failover Services

- On declaration of a disaster, Company will perform the steps necessary to restart and validate the database on the target DR server and make it the primary database, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the primary server, database administration of the database will be as per the administrative, support, backup and monitoring services as defined for the primary database.

Database Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The database administrator will assist the operating systems administrator reestablish database replication back to the target DR server.
- Database server Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Database Software Licensing

- Procurement of database software and licensing for current version on current operating system,
- including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the database
- Procurement of current software maintenance where applicable

OS Management or OS Level Replication Software, Infrastructure and Management
Management of the underlying operating system of the target DR server to maintain it to the same level as the primary database server is required.
This can be accomplished through manual management of the operating system or through OS based replication software.

600144 Microsoft SQL Database DR management via log shipping

Company's Responsibilities and Included Features

General
Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of a Microsoft SQL Database in a Recovery Site acting as a failover database.
Replication of the database binaries and non database file systems from the primary server to the target DR server is to be provided through the use of server to server replication software and requires an OS replication Service Item which will perform the replication.
Replication of the databases will be accomplished through the use of the native SQL Server replication services (Log shipping)
Company shall develop and maintain Disaster Recovery Failover Procedures. These procedures will be available at the Recovery Site.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR database is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Database Software Patch Management

- Monthly reviews of critical patches
- Up to quarterly routine review same-version patch analysis and application
- Periodic next version upgrade analysis and recommendations
- Application of updates and patches during approved maintenance windows
- Major or Point Release Upgrades.
- Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

SQL Replication Management
Configuration of replication policies
Monitoring of replication services
Diagnosis of replication incidents
Troubleshooting of replication incidents.

Database Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of failover tests per year is referenced in Pricing Parameters.
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster occur during a test, the data will be as old as the

data was when testing began.

Database Failover Services

- On declaration of a disaster, Company will perform the steps necessary to restart and validate the database on the target DR server and make it the primary database, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the primary server, database administration of the database will be as per the administrative, support, backup and monitoring services as defined for the primary database.

Database Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The database administrator will assist the operating systems administrator reestablish database replication back to the target DR server.
- Database server Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Database Software Licensing

- Procurement of database software and licensing for current version on current operating system,
- including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the database
- Procurement of current software maintenance where applicable

OS Management or OS Level Replication Software, Infrastructure and Management

Management of the underlying operating system of the target DR server to maintain it to the same level as the primary database server is required.
This can be accomplished through manual management of the operating system or through OS based replication software.

600145 Microsoft SQL database DR management - software/hypervisor based replication

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of a Microsoft SQL Database in a Recovery Site acting as a failover database.

Replication of the database binaries and non-database file systems from the primary server to the target DR server is to be provided through the use of Hypervisor and/or Third party appliations to replicate the whole database server, including operating system, database binaries and data.

Requires a Software of Hypervisor replication Service Item which will perform the replication.

Company shall develop and maintain Disaster Recovery Failover Procedures. These procedures will be available at the Recovery Site.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR database is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Database Software Patch Management

- Monthly reviews of critical patches
- Up to quarterly routine review same-version patch analysis and application
- Periodic next version upgrade analysis and recommendations
- Application of updates and patches during approved maintenance windows
- Major or Point Release Upgrades.
- Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Database Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of failover tests per year is referenced in Pricing Parameters.
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster occur during a test, the data will be as old as the data was when testing began.

Database Failover Services

- On declaration of a disaster, Company will perform the steps necessary to restart and validate the database on the target DR server and make it the primary database, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the primary server, database administration of the database will be as per the administrative, support, backup and monitoring services as defined for the primary database.

Database Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and

return service back to the Primary Site.

- The database administrator will assist the operating systems administrator reestablish database replication back to the target DR server.
- Database server Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Database Software Licensing

- Procurement of database software and licensing for current version on current operating system,
- including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the database
- Procurement of current software maintenance where applicable

OS Management or OS Level Replication Software, Infrastructure and Management

Management of the underlying operating system of the target DR server to maintain it to the same level as the primary database server is required.
This can be accomplished through manual management of the operating system or through OS based replication software.

600147 Oracle database disaster recovery from SAN replication

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of an Oracle Database in a Recovery Site acting as a failover database.
Replication of the database binaries and non-database file systems from the primary server to the target DR server is to be provided through the use of SAN replication of the whole database server, including operating system, database binaries and data.
Replication of the databases will be accomplished through the use of SAN replication services.
Requires a SAN replication Service Item which will perform the replication.
Company shall develop and maintain Disaster Recovery Failover Procedures. These procedures will be available at the Recovery Site.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time,

backwards from the point of disaster.

- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR database is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Database Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of failover tests per year is referenced in Pricing Parameters.
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster occur during a test, the data will be as old as the data was when testing began.

Database Failover Services

- On declaration of a disaster, Company will perform the steps necessary to restart and validate the database on the target DR server and make it the primary database, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the primary server, database administration of the database will be as per the administrative, support, backup and monitoring services as defined for the primary database.

Database Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The database administrator will assist the operating systems administrator reestablish database replication back to the target DR server.
- Database server Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying

them out, in response to a series of identified risks, with the objective of restoring normal business operation

SAN Replication Infrastructure, Software and Licensing

- Provisioning of SAN replication infrastructure (source and destination).
- Provisioning of SAN replication software and licensing for current version of replication software/infrastructure
- Procurement of current hardware and software maintenance where applicable

SAN Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

600148 Microsoft SQL database disaster recovery from SAN replication

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of a Microsoft SQL Database in a Recovery Site acting as a failover database.

Replication of the database binaries and non-database file systems from the primary server to the target DR server is to be provided through the use of SAN replication of the whole database server, including operating system, database binaries and data.

Replication of the databases will be accomplished through the use of SAN replication services.

Requires a SAN replication Service Item which will perform the replication.

Company shall develop and maintain Disaster Recovery Failover Procedures. These procedures will be available at the Recovery Site.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR database is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Database Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of failover tests per year is referenced in Pricing Parameters.

- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster occur during a test, the data will be as old as the data was when testing began.

Database Failover Services

- On declaration of a disaster, Company will perform the steps necessary to restart and validate the database on the target DR server and make it the primary database, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the primary server, database administration of the database will be as per the administrative, support, backup and monitoring services as defined for the primary database.

Database Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The database administrator will assist the operating systems administrator reestablish database replication back to the target DR server.
- Database server Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

SAN Replication Infrastructure, Software and Licensing

- Provisioning of SAN replication infrastructure (source and destination).
- Provisioning of SAN replication software and licensing for current version of replication software/infrastructure
- Procurement of current hardware and software maintenance where applicable

SAN Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

600305 Oracle Database Management - Configuration DB

Company's Responsibilities and Included Features

Oracle Database Administration

Description

This services is designed to provide Oracle database support for small, low transactional databases, like, application configuration databases, where the expectation is that the database requires minimal intervention to maintain the stability of the database.

Database Incident Triage and Troubleshooting

- Triage of database system incidents
- Troubleshooting of database system incidents
- Engagement of Oracle support
- Document user issues and database system errors

Database Monitoring

Configuration of database monitoring thresholds and parameters

- Monitoring of key metrics including:
- Database availability
- Space usage
- Blocking locks
- Concurrent sessions

Database Backup Management

- Configuration of database backup
- Monitoring of database backup status
- Rectification and resubmission of failed backup jobs as appropriate
- Adhoc backup or restore on request, limited to four per year
- Quarterly test restores

Database Software Patch Management

- Review of patches upon request or for specific bugs or issues
- Application of updates and patches during approved maintenance windows

Database Management Documentation

- Document applicable database administration procedures

Database Security Management

User creation and security maintenance
Database encryption and audit management where appropriate

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Database Software Licensing

- Procurement of database software and licensing for current version on current operating system,
- including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the database
- Procurement of current software maintenance where applicable

Third Party Application Dependency Management

- Management of third party application interface to the database

Database Schema and Content Management

- Development and/or customization of database schema
- Content management

Database Upgrades

Major or Point Release Upgrades - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

The following areas of Oracle database support are not included but can be provided on a time and material basis:

Database configuration and tuning

The following areas of Oracle database support are not included but can be provided on a time and material basis:

- Table and index storage parameters
- Table and index fragmentation
- Instance and database configuration options
- Oracle Net configuration and maintenance
- Optimizer statistics (tables, indexes, histograms and system statistics
- Concurrency (table/row locks)
- RAC management and support
- Disaster recovery support
- Database software configuration
- Physical and logical disk layout
- Database instance creation
- New database provisioning
- Backup and disaster recovery design strategies based on business needs
- Repository database creation for reporting or other peripheral tools creation
- Redistribution of data files
- Schema changes
- Query/explain plan analysis
- Memory utilization/configuration

600313 Microsoft SQL Server Administration Support

SQL Server Support*

* Microsoft SQL Server Administration Support is limited to number of hours per month as contracted.

SQL Server Administration Support provides qualified resources to support Microsoft SQL server. This includes the following areas within the SQL server suite of applications:

SQL Server Database

Setup

- Installation, setup and configuration of new database instances
- Adding new databases to existing SQL instances
- Setup SQL clustering

Support of:

- Transaction log maintenance
- Memory utilization/configuration
- Transaction log files
- Table and index storage parameters
- Table and index fragmentation
- Database storage parameters
- Instance and database configuration options
- Connectivity
- Table statistics
- Database issues such as table locks/record contention
- Database clusters
- SQL Backup administration
- SQL database security administration

Review and/or make recommendations within the following areas:

- Database software configuration
- Physical and logical disk layout
- Backup and disaster recovery design strategies based on business needs
- Repository database creation for reporting or other peripheral tools creation
- Redistribution of data files

SQL Server Reporting Services (SSRS)

Support the following areas within SSRS:

- Report Server Web Service
- Reporting Windows Service

- Reporting Services Log Files
- SSRS application support
- Monitoring Report Server Availability and Performance

SQL Server Integration Services (SSIS)

Support the following areas within SSIS:

- Integration Windows Service
- Integration Services Log Files
- SSIS application support

SQL Server Analysis Services (SSAS)

Support the following areas within SSAS:

- Object deployment
- Object impact analysis, starting and reprocessing
- Batch processing management
- SSAS application support

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Engagement of software providers Help Desk support (requires Client to have a support contract with the software provider)
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues
- Provide client with updates
- Document user issues and system errors

Database Instance Monitoring

- Configuration of database instance monitoring thresholds and parameters
- Monitoring and reporting of key metrics including: Database availability and SQL Services

SQL Server Security Management

- User creation and security maintenance
- Database authentication management via SQL authentication
- Database encryption management where appropriate

SQL Server Software Patch Management

- Reviews of critical patches
- Periodic next version upgrade analysis and recommendations

- Application of updates and patches during approved maintenance windows
- Major or Point Release Upgrades.
    - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Custom Object Change Management

- Migration of customizations through development, test, QA environments (as applicable) through to production
- Change control

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Software Licensing

- Procurement of software and licensing for current version on current operating system,
- including any user or processor access licensing
- Providing software media for installation, maintenance and configuration of the SQL Server
- Procurement of current software maintenance where applicable

Operating System Administration

System administration of the server operating system including:

- Operating system configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks

End User Support and Management

- Support of non-super users
- Application functional support
- Content or data related support or management
- End user client software support

Database Schema and Content Management

- Development and/or customization of database schema
- Content management

Reporting Services Development

- Development and maintenance of reports, scripts and objects
- Diagnosis and troubleshooting of processing failures related to content or reports, scripts and objects

Integration Services Development

- Development and maintenance of SSIS packages and the integration with items outside of SQL (i.e. applications, etc.)
- Triage and troubleshooting of processing failures related to items outside of SQL (i.e. applications, etc.)
- Third Party Application Dependency/Relationship Management
- Management of third party application interface to the database

Third Party Application Dependency Management

- Management of third party application interface to the database

600528 Oracle database disaster recovery from SAN replication Discount

Company's Responsibilities and Included Features

Company agrees to provide a per unit discount to ItemID 600147-Oracle database disaster recovery from SAN replication in the amount shown in the Unit Price of the Monthly Fees for this ItemID for each Oracle database disaster recovery from SAN replication instance, up to and including a quantity of Forty Six (46) instances.

600529 Microsoft SQL database disaster recovery from SAN replication Discount

Company's Responsibilities and Included Features

Company agrees to provide a per unit discount to ItemID 600148-Microsoft SQL database disaster recovery from SAN replication in the amount shown in the Unit Price of the Monthly Fees for this ItemID for each Microsoft SQL database disaster recovery from SAN replication instance, up to and including a quantity of Twenty Eight (28) databases.

601393 Microsoft Dynamics 365 SQL Database Refresh

Company's Responsibilities and Included Features

Database Refresh

A Microsoft Dynamics 365 (D365) database refresh is defined as the process of exporting a D365 database to a file and then reimport that file into another non-production instance of the application.

This process can be only be used to refresh a non-production target environment.

The Company will execute the export and import process on request or on a predefined schedule, which will include the following:

- The target environment will be unavailable during the export / import process
- Export the bacpac file via Microsoft Life Cycle Services LCS
- Import the bacpac file on to the target D365 non-production instance
- Execute the following post-restore steps
  - DB Permission Updates
  - DB Synchronization
- Execute Client defined post-restore steps
- Notification of completion of the export/import process

The service is for one D365 database refresh per month

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client Defined Post-restore Steps

- Provide details of post-restore steps to be executed by Company

Database Refresh Request

- Database refresh must be scheduled at least 3 business days in advance.
- Database refresh request must originate from a user approved to request a refresh to the target database.
- Users must log out of the target application/database prior to scheduled start of refresh.

601456

Company's Responsibilities and Included Features

Oracle Database Support*

Oracle database support provides qualified resources to manage Oracle databases within the monthly bucket of hours as contracted.

This includes the following areas within the Oracle database:

Management

- Transaction log maintenance
- Memory utilization/configuration
- Transaction log files
- Table and index storage parameters
- Table and index fragmentation
- Database storage parameters
- Instance and database configuration options
- Connectivity
- Table statistics
- Database issues such as table locks/record contention
- Database cluster management
- Database backup administration
- Database security administration
- Database patching
- Oracle RAC

Review and/or make recommendations within the following areas:

- Database software configuration
- Physical and logical disk layout
- Backup and disaster recovery design strategies based on business needs
- Repository database creation for reporting or other peripheral tools creation
- Redistribution of data files
- Schema changes

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Engagement of software providers Help Desk support (requires Client to have a support contract with the software provider)
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues

Provide client with updates
- Document user issues and system errors

*** Oracle Database Support is limited to the number of hours per month as contracted.**

Oracle Database Support is provided by non-USA resident resources (offshore)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Procurement of database software and licensing for the current version of the current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance, and configuration of the database
- Procurement of current software maintenance where applicable

Server Operating System Administration

System administration of the server operating system including:

- Operating system configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks

601457

Company's Responsibilities and Included Features

Oracle Database Support*

Oracle database support provides qualified resources to manage Oracle databases within the monthly bucket of hours as contracted.

This includes the following areas within the Oracle database:

Management

- Transaction log maintenance
- Memory utilization/configuration
- Transaction log files
- Table and index storage parameters
- Table and index fragmentation
- Database storage parameters
- Instance and database configuration options
- Connectivity
- Table statistics
- Database issues such as table locks/record contention
- Database cluster management
- Database backup administration
- Database security administration
- Database patching
- Oracle RAC

Review and/or make recommendations within the following areas:

- Database software configuration
- Physical and logical disk layout
- Backup and disaster recovery design strategies based on business needs
- Repository database creation for reporting or other peripheral tools creation

- Redistribution of data files
- Schema changes

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Engagement of software providers Help Desk support (requires Client to have a support contract with the software provider)
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues
- Provide client with updates
- Document user issues and system errors

*** Oracle Database Support is limited to the number of hours per month as contracted.**

Oracle Database Support is provided by USA resident resources (onshore)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Procurement of database software and licensing for the current version of the current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance, and configuration of the database
- Procurement of current software maintenance where applicable

Server Operating System Administration

System administration of the server operating system including:

- Operating system configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks

601464

Company's Responsibilities and Included Features

Oracle Database Support*

Oracle database support provides qualified resources to manage Oracle databases within the monthly bucket of hours as contracted.

This service is limited to support for the following items in the Client s BID 2019-22

- ITEM 3 Oracle Database Enterprise Edition Named User Single Server CSI #3225649 (QTY 40)
- ITEM 4 Change Management Pack Processor Perpetual CSI #3335254 (QTY 4)
- ITEM 5 Oracle Database Enterprise Edition Named User Perpetual CSI #3335254 (QTY 20)
- ITEM 6 Oracle Diagnostics Pack Processor Perpetual CSI #3335254 (QTY 4)
- ITEM 7 Oracle Real Application Clusters Processor Perpetual CSI #3335254 (QTY 4)
- ITEM 8 Oracle Tuning Pack Processor Perpetual CSI #3335254 (QTY 4)
- ITEM 9 Oracle Database Enterprise Edition Processor Perpetual CSI #3643257 (QTY 2)
- ITEM 10 Oracle Real Application Clusters Processor Perpetual CSI #3643257 (QTY 2)
- ITEM 11 Oracle Database Enterprise Edition Processor Perpetual CSI #13553707 (QTY 2)
- ITEM 12 Oracle Database Enterprise Edition Processor Perpetual CSI #13553707 (QTY 1)
- ITEM 14 Oracle Database Enterprise Edition Processor Perpetual CSI #13856383 (QTY 2)

Oracle Database Support includes the following areas within the Oracle database:

Management

- Transaction log maintenance
- Memory utilization/configuration
- Transaction log files
- Table and index storage parameters
- Table and index fragmentation
- Database storage parameters
- Instance and database configuration options
- Connectivity
- Table statistics
- Database issues such as table locks/record contention
- Database cluster management
- Database backup administration
- Database security administration
- Database patching
- Oracle RAC

Review and/or make recommendations within the following areas:

- Database software configuration
- Physical and logical disk layout
- Backup and disaster recovery design strategies based on business needs
- Repository database creation for reporting or other peripheral tools creation
- Redistribution of data files
- Schema changes

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Engagement of software providers Help Desk support (requires Client to have a support contract with the software provider)
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues
- Provide client with updates
- Document user issues and system errors

Oracle Database Support is provided by non-USA resident resources (offshore)

* Oracle Database Support is limited to the number of hours per month as contracted for this ItemID. Unused hours will not roll over to subsequent months.

Oracle Database Support Prioritization and Engagement Objectives

- Company will provide support to the Client s IT group or users for Oracle Database Support through question and issue submission through incident tickets submitted to and administered by Company s help desk, prioritized as follows:

Priority	Definition	Support Hours	Engagement Objective during Support Hours
1	One or more business critical application functions is impeding the customer s ability to perform business.	Monday-Friday, 8am-5pm CST/CDT	30 minutes
2	One or more business critical application functions are degraded and is impacting the customer s ability to perform business.	Monday-Friday, 8am-5pm CST/CDT	2 hours
3	The incident has a medium impact on the customer's ability to perform business.	Monday-Friday, 8am-5pm CST/CDT	4 hours

4	The incident has a minor impact on the customer's ability to perform business.	Monday-Friday, 8am-5pm CST/CDT	24 hours
5	The incident has no impact to the customer s ability to perform business.	Monday-Friday, 8am-5pm CST/CDT	48 hours

- Oracle Database Support will be provided on a best effort basis for any time outside of the designated support hours, unless agreed upon in advance by both parties

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Procurement of database software and licensing for the current version of the current operating system, including any user or processor access licensing
- Providing software media for installation, maintenance, and configuration of the database
- Procurement of current software maintenance where applicable

Server Operating System Administration

System administration of the server operating system including:

- Operating system configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks

601483

Company's Responsibilities and Included Features

Azure Database for MariaDB Management - One Region - Base provides the basis for a Client s instance of Azure Database for MariaDB management and requires ItemID 601484, Azure Database for MariaDB Management - One Region - Database which captures the number of individual databases within the Azure Database for MariaDB platform that are to be managed under this ItemID.

Azure Database for MariaDB Administration

Azure Database administration within one Azure region including:

- Initial database assessment and performance adjustments
- New database provisioning
- Configuration of database instance monitoring thresholds and parameters

Azure Database for MariaDB Monitoring

- Database availability monitoring
- Availability and Reliability management (Azure PaaS SLA 99.99%)
- Performance monitoring and tuning

Incident Triage and Troubleshooting

- Advanced DBA support for database issues and performance tuning/recommendations
- Escalate issues to Microsoft as needed
- Document issues and errors
- Troubleshooting using slow query log (limited by Azure to 7 days)
- Manage security settings based on best practices

Database Security Management

- User creation and security maintenance

Database authentication management
- Database encryption management where appropriate

Azure Database for MariaDB Management Documentation

- Document applicable Azure Database for MariaDB administration procedures and policies

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Content Management and Development

- Database content management
- Database development
- Configuration documentation (if applicable)

Microsoft Azure Subscription

- Azure subscription and resources needed to support Azure Database for MariaDB
- Backups of proprietary data (Microsoft platform provided)
- Utilize Company Microsoft Cloud Services Provider (CSP) subscription or provide Company access to Client subscription
- Provide Azure Private Endpoint for remote administration connectivity

Application and Dependencies

- Application and content updates
- Third-party application dependencies

Client Access Licensing

- End-user access licensing of OS or application, if applicable

End User Support

- Support of non-expert users (Typically refers to non-IT department staff or application end users

601484

Company's Responsibilities and Included Features

Deliver per database management for the Client s Azure Database for MariaDB as described under required ItemID 601483 Azure Database for MariaDB Management One Region - Base.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

None

601568 Azure SQL Service Management - One Region Base

Company's Responsibilities and Included Features

Azure SQL Database Service Management One Region - Base provides the basis for management of a Client s Azure SQL Service and requires Client subscription to Company ItemID 601572, Azure SQL Database Management - Type 1 which captures the number of individual databases within the Azure SQL Service that are to be managed under this ItemID. Azure SQL Database Service Management One Region Base covers single database and elastic pool database types.

Azure SQL Service Monitoring

- Availability and reliability monitoring

Incident Triage and Troubleshooting

- Diagnosis of service incidents
- Triage of service incidents
- Troubleshoot and work to resolve service incidents
- Document service incidents
- Escalate incidents to Microsoft as needed

Database Security Administration

- Database firewall settings
- Configuration of security auditing

Elastic Pool Management

- Adding or removing databases to an elastic pool
- Scaling up an elastic pool - make changes as requested via service ticket submission
- Scaling down an elastic pool make changes as requested via service ticket submission
    - Limited to 1 change per quarter

Azure SQL Service Administration Documentation

- Document applicable Azure SQL service administration procedures and policies

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Subscription to Company ItemID 601572, Azure SQL Database Management Type 1

Microsoft Azure Subscription

- Azure subscription and resources needed to support Azure SQL Database
- Provide Azure monitoring resources Azure Monitor and Log Analytics for service monitoring
- Provide Company access to subscriptions
- Provide Azure Private Endpoint for remote administration connectivity

Scaling Backup

- Backups of database (Azure platform provided)
- Provide backup retention requirements

Security & Audit Requirements

- Provide audit requirements
- Azure resources for audit logging

Application and Dependencies

- Application and content updates
- Third-party application dependencies

End User Support

- Support of non-Expert Users (typically refers to non-IT department staff or application end users)

601572 Azure SQL Database Management - Type 1

Company's Responsibilities and Included Features

Deliver per database administration for the Client s Azure SQL Database. Requires Client subscription to Company ItemID 601568 Azure SQL Database Service Management One Region Base. Azure SQL Database Management Type 1 provides management of an Azure SQL database on a single database or an elastic pool. Databases on Azure SQL Managed Instance are not in scope of this service.

Azure SQL Service Backup

- Configuration of database backup retention policies
- Provide support for backup restores utilizing the Azure provided backup service

Azure SQL Database Monitoring

- Availability monitoring
- Performance monitoring
- Events monitoring
- Azure SQL Database Reviews
- Periodic database performance and health reviews

Scaling

- OneNeck will monitor and provide quarterly recommendations on compute sizing changes
- Reconfigure autoscaling for serverless databases as requested via service ticket submission
- Monitor for critical capacities and provide recommendations
- Scaling up - make changes as requested via service ticket submission
- Scaling down make changes as requested via service ticket submission
    - Limited to 1 change per quarter

Incident Triage and Troubleshooting

- Diagnosis of database incidents
- Triage of database incidents

- Troubleshoot and work to resolve database incidents
Document database incidents
- Escalate incidents to Microsoft as needed

Database Security Administration

- User creation and security maintenance
- Database authentication management
- Configuration of security auditing
- Database encryption management

Azure SQL Database Administration Documentation

- Document applicable Azure SQL database administration procedures and policies

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Subscription to Company ItemID 601568 Azure SQL Database Service Management - One Region Base

Content Management and Development

- Database content management
- Database development
- Provide Company access to subscriptions

Microsoft Azure Subscription

- Azure subscription and resources needed to support Azure SQL Database
- Provide Azure monitoring resources Azure Monitor and Log Analytics for service monitoring
- Provide Company access to subscriptions
- Provide Azure Private Endpoint for remote administration connectivity

Scaling

- Autoscaling or frequent scaling of compute requires an automated process to be developed as a separate project
- Application management, including any activities required to make resource changes (scale up, scale down)

Security & Audit Requirements

- Provide audit requirements
- Azure resources for audit logging
- Azure Active Directory management

Backup

- Provide backup retention requirements

Application and Dependencies

- Application and content updates
- Configuration documentation specific to application (if applicable)
- Third-party application dependencies impacted by scaling changes

End User Support

- Support of non-Expert Users (typically refers to non-IT department staff or application end users)

601849 Azure SQL Managed Instance Management - One Region - Base

Azure SQL Managed Instance Management - One Region - Base provides the basis for management of a Client s Azure SQL Managed Instance and requires Client subscription to Company ItemID 601850 Azure SQL Database Management - Type 2 which captures the number of individual databases within the Azure SQL Service that are to be managed under this ItemID.
Company's Responsibilities and Included Features

Azure SQL Managed Instance Monitoring

- Configuration of instance monitoring thresholds and parameters
- Availability and reliability monitoring
- Performance monitoring
- SQL Agent job monitoring and escalation
- Events monitoring

Scaling

- Company will monitor and provide quarterly recommendations on compute sizing changes
- Monitor for critical capacities and provide recommendations
- Scaling up - make changes as requested via service ticket submission
- Scaling down make changes as requested via service ticket submission
    - Limited to 1 change per quarter

Incident Triage and Troubleshooting

- Diagnosis of service incidents
- Triage of service incidents
- Troubleshoot and work to resolve service incidents
- Document service incidents
- Escalate incidents to Microsoft as needed

Database Security Administration

- User creation and security maintenance
- Instance network security settings
- Configuration of security auditing
- Database encryption management

Azure SQL Database Administration Documentation

- Document applicable Azure SQL Managed Instance administration procedures and policies

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Subscription to Company ItemID 601850, Azure SQL Database Management Type 2

Custom SQL Agent Jobs

- Development and troubleshooting of custom SQL Agent jobs (as provided above, Company will escalate incidents only)
- Provide monitoring escalation procedure for custom SQL Agent jobs

Microsoft Azure Subscription

- Azure subscription and resources needed to support Azure SQL Managed Instance
- Provide Azure monitoring resources Azure Monitor and Log Analytics for service monitoring
- Provide Company access to subscriptions
- Provide Azure Private Endpoint for remote administration connectivity

Scaling

- Autoscaling or frequent scaling of compute requires an automated process to be developed as a separate project
- Application management, including any activities required to make resource changes (scale up, scale down)

Security & Audit Requirements

- Provide audit requirements
- Provide Azure resources for audit logging
- Provide backup retention requirements to Company

Backup

- All database backups are out of scope of Company provided services (automated backups are available via the Azure platform)
- Provide backup retention requirements to Company

Application and Dependencies

- Perform application and content updates
- Provide third-party application dependencies

End User Support

- Support of non-Expert Users (typically refers to non-IT department staff or application end users)

601850 Azure SQL Database Management - Type 2

Azure SQL Database Management Type 2 provides management of an Azure SQL database on an Azure SQL Managed Instance. Databases on Azure SQL Database or in elastic pools are not in scope of this service.

Company's Responsibilities and Included Features

Azure SQL Database Management

- Manage
    - able and index storage parameters
    - Table and index fragmentation
    - Database storage parameters
    - Database configuration options

        - Table statistics
        - Database issues such as table locks/record contention
    - Deploy schema changes

Azure SQL Database Backup

- Configuration of database backup retention policies
- Provide support for backup restores utilizing the Azure provided backup service
- Perform ad hoc backup or restore on request, limited to four per year

Azure SQL Database Monitoring

- Availability monitoring
- Events monitoring

Azure SQL Database Reviews

- Periodic database performance and health reviews

Incident Triage and Troubleshooting

- Diagnosis of service incidents
- Triage of service incidents
- Troubleshoot and work to resolve service incidents
- Document service incidents
- Escalate incidents to Microsoft as needed

Database Security Administration

- User creation and security maintenance
- Database authentication management

Azure SQL Database Administration Documentation

- Document applicable Azure SQL database administration procedures and policies

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Subscription to Company ItemID 601849 Azure SQL Managed Instance Management - One Region Base

Content Management and Development

- Database content management
- Database development

Microsoft Azure Subscription

- Provide Azure subscription and resources needed to support Azure SQL Database
- Provide Azure monitoring resources
- Provide resources for Azure Monitor and Log Analytics for service monitoring
- Provide Company access to subscriptions
- Provide Azure Private Endpoint for remote administration connectivity

Security & Audit Requirements

- Provide audit requirements
- Provide Azure resources for audit logging
- Provide Azure Active Directory management

Backup

- Provide backup retention requirements to Company

Application and Dependencies

- Perform application and content updates
- Provide configuration documentation specific to application (if applicable)
- Manage third-party application dependencies impacted by scaling changes

End User Support

- Support of non-Expert Users (typically refers to non-IT department staff or application end users)

602392 PostgreSQL Server Instance Administration - PLACEHOLDER

This is a placeholder for a Company service to deliver PostgreSQL administration that still needs to be developed and rolled out to Client by Company.

Contracting this ItemID does not imply any Company commitment to the delivery of this service in any specific time span.

A subsequent Change Order for this service will be issued to update the scope of services for this service.

602393 PostgreSQL Database Administration - Type 2 - PLACEHOLDER

This is a placeholder for a Company service to deliver PostgreSQL administration that still needs to be developed and rolled out to Client by Company.

Contracting this ItemID does not imply any Company commitment to The delivery of this service in any specific time span.

A subsequent Change Order for this service will be issued to update the scope of services for this service.

603769 Microsoft SQL Server Instance Administration - Base

Company's Responsibilities and Included Features

This service provides the basis for Microsoft SQL Server Instance Administration and requires ItemID 603770 Microsoft SQL Server Instance Administration Core which provides for scalable management based upon the number of physical cores or virtual CPUs

Database Instance Administration

- An instance of SQL is defined as the set of Microsoft SQL Server software or set of SQL server binaries loaded on a single instance of the operating system.
- Multiple instances of MS SQL may occur on a single instance of a MS Windows OS

Database Instance Monitoring

- Configuration of database instance monitoring thresholds and parameters
- Monitoring and reporting of key metrics including:
- Database availability
- SQL Services

Database Incident Diagnosis and Troubleshooting

- Diagnosis of database system incidents
- Troubleshoot and work to resolve database system incidents
- Engagement of database software providers help desk support
- Document user issues and database system errors

SQL Database Security Management

- User creation and security maintenance
- Database authentication management via SQL authentication
- Database encryption management where appropriate

Database Software Patch Management

- Monthly reviews of critical patches
- Up to quarterly routine review same-version patch analysis and application
- Periodic next version upgrade analysis and recommendations
- Application of updates and patches during approved maintenance windows
- Major or Point Release Upgrades.
-
    - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

SQL Database Administration

SQL database administration is defined as the tasks to maintain the individual databases on the SQL instance.

These tasks includes administration and tuning the following areas within the database:

General Database Administration

- Transaction log maintenance
- Memory utilization/configuration
- Transaction log files
- Table and index storage parameters
- Table and index fragmentation
- Database storage parameters
- Database configuration options
- Table statistics
- Database issues such as table locks/record contention
- Deployment of schema changes

Review and/or make recommendations* within the following areas:

- Physical and logical disk layout
- New database provisioning
- Backup and disaster recovery design strategies based on business needs
- Repository database creation for reporting or other peripheral tools creation
- Redistribution of data files

* Implementation of recommendations will be handled on a per project time and material basis

Database Incident Diagnosis and Troubleshooting

- Diagnosis of database system incidents
- Troubleshooting of database system incidents
- Engagement of database software providers help desk support
- Document user issues and database system errors

Database Monitoring

- Configuration of database monitoring thresholds and parameters
- Monitoring and reporting of key metrics including:
-
    - Database availability
    - Space usage

Database Backup Administration

- Configuration of database backup
- Monitoring of database backup status
- Rectification and resubmission of failed backup jobs as appropriate
- Adhoc backup or restore on request, limited to four per year
- Quarterly test restores

SQL Database Security Administration

- User creation and security maintenance
- Database authentication management via SQL authentication
- Database encryption management where appropriate

Database Cloning

- Cloning/copying/refreshing of databases to a non-production environment for system testing, training, or development.
- Number of clones per database is limited to one (1) per month
- Database management documentation
- Document applicable database administration procedures

Expert User Technical Support*

Expert-to-expert helpdesk support:

- 24 x 7 technical support for priority 1 and 2 incidents
- 8 am to 5 pm technical support for priority 3, 4 and 5 incidents

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

SQL Always on Availability Group (AOAG) Administration

- Contracting for Company provided SQL AOAG administration if SQL AOAG is used

SQL Failover Cluster Instance (FCI) Administration

- Contracting for Company provided SQL FCI administration if SQL FCI is used

Database Software Licensing

- Procurement of database software and licensing for current version on current operating system,
- including any user or processor access licensing
- Procurement of current software maintenance where applicable

Backup Infrastructure (Tape or Disk Based) (if server is required to be backed up)

Backup system to enable backup of data from this server to tape or disk:

- Backup server and agent licensing, with available disk storage and tape media if required
- Management of backup system
- Tape storage (on-site or off-site, if applicable)

or

- Contracted usage of the Company backup service

Third Party Application Dependency Management.

- Management of third party application interface to the database

Domain User Administration

Provisioning of Active Directory domain users including:

- Group membership updates
- Password resets
- Termination of Active Directory domain users
- No change notice required for user administration

Database schema and content management

- Development and/or customization of database schema
- Content management

603770 Microsoft SQL Server Instance Administration - Cores

Company's Responsibilities and Included Features

This Microsoft SQL Server Instance Administration - Cores SKU provides scalable management based upon the number of physical cores or virtual CPUs for SKU 603769 Microsoft SQL Server Instance Administration - Base

Provide Microsoft SQL Server instance and database administration as documented in ItemID 603769 up to the contracted physical core or virtual CPU count for this ItemID 603770

603771 Microsoft SQL Server AOAG Administration

Company's Responsibilities and Included Features

This service provides for the additional Microsoft SQL Server instance administration when SQL instances are in Always ON Availability Groups (AOAG) and requires ItemID 603769 Microsoft SQL Server Instance Administration - Base & ItemID 603770 Microsoft SQL Server Instance Administration Core.

AOAG Administration

Windows Cluster Server Monitoring

- Install Company licensed monitoring agents where applicable
- Configure monitoring thresholds and parameters
- Monitor cluster status and health, including:

Cluster group status
- Cluster service status
- Cluster resource state
- Cluster node state

Cluster Failover Administration

- Manual failover administration where needed
- Dependency configuration

Windows Cluster Server Patch Administration

- Providing sequential node patching as a part of the Windows Server patching provide for within the OS administration as contracted separately

Cluster Server Incident Triage and Troubleshooting

- Triage of Windows Cluster Server and AOAG incidents
- Troubleshoot and work to resolve server Cluster Server incidents
- Document Cluster Server system issues and errors

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as a Client designated person with an in-depth application or system knowledge who is a designated Client contact for initiating or escalating incidents to Company limited to 5 total defined experts or 5% of the Client's staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating System Managed Services

Contract for Company OS Managed Services for the Windows Servers that are part of the AOAG

603868 Microsoft SQL Server Failover Cluster Instance Administration

Company's Responsibilities and Included Features

This service provides for the additional Microsoft SQL Server instance administration when SQL instances are in a Failover Cluster Instance (FCI)

FCI Administration

- Cluster quorum administration
- Cluster properties configuration
- Node properties configuration

Windows Cluster Server Monitoring

- Install Company licensed monitoring agents where applicable
- Configure monitoring thresholds and parameters
- Monitor cluster status and health, including:
    - Cluster group status

- Cluster service status
- Cluster resource state
- Cluster node state

Cluster Failover Administration

- Manual failover administration

Windows Cluster Server Patch Administration

- Providing sequential node patching as a part of the Windows Server patching provide for within the OS administration as contracted separately

Cluster Server Incident Triage and Troubleshooting

- Triage of Windows Cluster Server and FCI incidents
- Troubleshoot and work to resolve server Cluster Server incidents
- Document Cluster Server system issues and errors

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as a Client designated person with an in-depth application or system knowledge who is a designated Client contact for initiating or escalating incidents to Company limited to 5 total defined experts or 5% of the Client's staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating System Managed Services

- Contract for Company OS Managed Services for the Windows Servers that are part of the FCI

Active Directory Administration

- Configuration of Failover Cluster virtual objects in Active directory and DNS security

603929 PostgreSQL Instance Administration - Base

Company's Responsibilities and Included Features

This service provides the basis for PostgreSQL Instance Administration and requires ItemID 603930 PostgreSQL Instance Administration Core which provides for scalable management based upon the number of cores

Database Instance Administration

- An instance of PostgreSQL is defined as the set of PostgrePostgreSQL software or set of PostgreSQL server binaries loaded on a single instance of the operating system.
- Multiple instances of PostgreSQL may occur on a single instance of Windows, Linux, Unix platform.

Database Instance Monitoring

- Configuration of database instance monitoring thresholds and parameters
- Monitoring and reporting of key metrics including:

Database availability
- PostgreSQL Services

Database Incident Diagnosis and Troubleshooting

- Diagnosis of database system incidents
- Troubleshoot and work to resolve database system incidents
- Engagement of database software providers help desk support
- Document user issues and database system errors

PostgreSQL Database Security Management

- User creation and security maintenance
- Database authentication management
- Database encryption management where appropriate

Database Software Patch Management

- Monthly reviews of critical patches
- Up to quarterly routine review same-version patch analysis and application
- Periodic next version upgrade analysis and recommendations
- Application of updates and patches during approved maintenance windows
- Major or Point Release Upgrades.
    - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

PostgreSQL Database Administration

PostgreSQL database administration is defined as the tasks to maintain the individual databases on the PostgrePostgreSQL instance.

These tasks includes administration and tuning the following areas within the database:

General Database Administration

- Transaction log maintenance
- Memory utilization/configuration
- Transaction log files
- Table and index storage parameters
- Table and index fragmentation
- Database storage parameters
- Database configuration options
- Table statistics
- Database issues such as table locks/record contention
- Deployment of schema changes

Review and/or make recommendations* within the following areas:

- Physical and logical disk layout
- New database provisioning
- Backup and disaster recovery design strategies based on business needs
- Repository database creation for reporting or other peripheral tools creation
- Redistribution of data files

* Implementation of recommendations will be handled on a per project time and material basis

Database Incident Diagnosis and Troubleshooting

- Diagnosis of database system incidents

- Troubleshooting of database system incidents
- Engagement of database software providers help desk support
- Document user issues and database system errors

Database Monitoring

- Configuration of database monitoring thresholds and parameters
- Monitoring and reporting of key metrics including:
    - Database availability
    - Space usage

Database Backup Administration

- Configuration of database backup
- Monitoring of database backup status
- Rectification and resubmission of failed backup jobs as appropriate
- Adhoc backup or restore on request, limited to four per year
- Quarterly test restores

PostgreSQL Database Security Administration

- User creation and security maintenance
- Database authentication management via PostgreSQL authentication
- Database encryption management where appropriate

Database Cloning

- Cloning/copying/refreshing of databases to a non-production environment for system testing, training, or development.
- Number of clones per database is limited to one (1) per month
- Database management documentation
- Document applicable database administration procedures

Expert User Technical Support*

Expert-to-expert helpdesk support:

- 24 x 7 technical support for priority 1 and 2 incidents
- 8 am to 5 pm technical support for priority 3, 4 and 5 incidents

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

High Availability

- OLTP Performance
- Data Migration
- Testing Systems in Parallel

PostgreSQL Cluster Instance Administration

- Fault Tolerance

Database Software Licensing

- If the PostgreSQL version is not the PostgreSQL Community version then,

- Procurement of database software and licensing for current version on current operating system including any user or processor access licensing
- Procurement of current software maintenance where applicable

Backup Infrastructure (Tape or Disk Based) (if server is required to be backed up)

Backup system to enable backup of data from this server to tape or disk:

- Backup server and agent licensing, with available disk storage and tape media if required
- Management of backup system
- Tape storage (on-site or off-site, if applicable)

or

- Contracted usage of the Company backup service

Third Party Application Dependency Management.

- Management of third party application interface to the database

Third Party Application Dependency Management

- Management of third-party application interface to the database

Database schema and content management

- Development and/or customization of database schema
- Content management

603930 PostgreSQL Instance Administration - Cores

Company's Responsibilities and Included Features

This PostgreSQL Instance Administration - Cores SKU provides scalable management based upon the number of cores for SKU 603929 PostgreSQL Instance Administration - Base

Provide PostgreSQL instance and database administration as documented in ItemID 603929 up to the contracted core count for this ItemID 603930

603931 PostgreSQL Cluster Administration

Company's Responsibilities and Included Features

This service provides for the additional PostgreSQL instance cluster administration for high availability of PostgreSQL environment. .

Cluster Administration

Windows/Linux/Unix Cluster Server Monitoring

- Install Company licensed monitoring agents where applicable
- Configure monitoring thresholds and parameters
- Monitor cluster status and health, including:
    - Cluster group status
    - Cluster service status
    - Cluster resource state
    - Cluster node state

Cluster Failover Administration

- Manual failover administration where needed
- Dependency configuration

Windows Cluster Server Patch Administration

- Providing sequential node patching as a part of the Windows/Linux/Unix Server patching provide for within the OS administration as contracted separately

Cluster Server Incident Triage and Troubleshooting

- Triage of Windows/Linux/Unix Cluster Server and PostgreSQL cluster incidents
- Troubleshoot and work to resolve server Cluster Server incidents
- Document Cluster Server system issues and errors

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as a Client designated person with an in-depth application or system knowledge who is a designated Client contact for initiating or escalating incidents to Company limited to 5 total defined experts or 5% of the Client's staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating System Managed Services

Contract for Company OS Managed Services for the servers that are any part of the cluster

603994 Microsoft SQL Server Instance Management

Company's Responsibilities and Included Features

Database Instance Management

- An instance of SQL is defined as the set of Microsoft SQL Server software or set of SQL server binaries loaded on a single instance of the operating system.
- Multiple instances of MS SQL may occur on a single instance of a MS Windows OS

Database Instance Monitoring

- Configuration of database instance monitoring thresholds and parameters
- Monitoring and reporting of key metrics including:
- Database availability
- SQL Services

Database Incident Diagnosis and Troubleshooting

- Diagnosis of database system incidents
- Troubleshoot and work to resolve database system incidents
- Engagement of database software providers help desk support
- Document user issues and database system errors

SQL Database Security Management

- User creation and security maintenance
- Database authentication management via SQL authentication
- Database encryption management where appropriate

Database Software Patch Management

- Monthly reviews of critical patches
- Up to quarterly routine review same-version patch analysis and application
- Periodic next version upgrade analysis and recommendations
- Application of updates and patches during approved maintenance windows
- Major or Point Release Upgrades.
    - Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Expert User Technical Support*

Expert-to-expert helpdesk support:

- 24 x 7 technical support for priority 1 and 2 incidents
- 8 am to 5 pm technical support for priority 3, 4 and 5 incidents

* An Expert User is defined as someone with in-depth application or system knowledge and a single point of contact for escalating incidents to Company. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

*** An Expert User is defined as a Client designated person with an in-depth application or system knowledge who is a designated Client contact for initiating or escalating incidents to Company limited to 5 total defined experts or 5% of the Client's staff, whichever is greater.**

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Database Software Licensing

- Procurement of database software and licensing for current version on current operating system,
- including any user or processor access licensing
- Procurement of current software maintenance where applicable

Backup Infrastructure (Tape or Disk Based) (if server is required to be backed up)

Backup system to enable backup of data from this server to tape or disk:

- Backup server and agent licensing, with available disk storage and tape media if required
- Management of backup system
- Tape storage (on-site or off-site, if applicable)

or

- Contracted usage of the Company backup service

604201 Microsoft SQL database disaster recovery using SQL AOAG replication

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of a Microsoft SQL Database in a Recovery Site acting as a failover database.
Replication of the databases will be accomplished through the use of Microsoft SQL AOAG replication services.
Company shall develop and maintain Disaster Recovery Failover Procedures. These procedures will be available at the Recovery

Site.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR database is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Database Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- One (1) failover tests per year is included in the service
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster occur during a test, the data will be as old as the data was when testing began.

Database Failover Services

- On declaration of a disaster, Company will perform the steps necessary to restart and validate the database on the target DR server and make it the primary database, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the primary server, database administration of the database will be as per the administrative, support, backup and monitoring services as defined for the primary database.

Database Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The database administrator will assist the operating systems administrator reestablish database replication back to the target DR server.
- Database server Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying

them out, in response to a series of identified risks, with the objective of restoring normal business operation

Microsoft SQL Database Administration

- Contract with Company to provide Microsoft SQL Server administration of all Microsoft SQL instances included in the DR environment

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

604419 Microsoft SQL Database Disaster Recovery from Hypervisor-based Replication

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the administration of a Microsoft SQL Database in a Recovery Site acting as a failover database.

Replication of the database binaries and non-database file systems from the primary server to the target DR server is to be provided through the use of hypervisor-based replication of the whole database server, including operating system, database binaries and data.

Requires a hypervisor-based replication Service Item which will perform the replication.

Company shall develop and maintain Disaster Recovery Failover Procedures. These procedures will be available at the Recovery Site.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR database is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Database Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of failover tests per year is referenced in Pricing Parameters.
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster occur during a test, the data will be as old as the data was when testing began.

Database Failover Services

- On declaration of a disaster, Company will perform the steps necessary to restart and validate the database on the target DR server and make it the primary database, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the primary server, database administration of the database will

be as per the administrative, support, backup and monitoring services as defined for the primary database.

Database Failback Services

- When the ability to provide services from the Primary Site is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the Primary Site.
- The database administrator will assist the operating systems administrator reestablish database replication back to the target DR server.
- Database server Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Hypervisor-based Replication Infrastructure, Software and Licensing

- Provisioning of hypervisor-based replication infrastructure (source and destination).
- Provisioning of hypervisor-based replication software and licensing for current version of replication software/infrastructure
- Procurement of current hardware and software maintenance where applicable

Hypervisor-based Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

604669 PostgreSQL Azure PaaS Server Administration - Base

Company's Responsibilities and Included Features

This service provides the basis for Azure PostgreSQL Server Administration and requires ItemID 604670 PostgreSQL Azure PaaS Service Administration Core, which provides for scalable management based upon the number of cores. PostgreSQL Azure PaaS Server Administration Base covers both Single and Flexible server options.

Database Service Monitoring

- Configuration of database service/cluster monitoring thresholds and parameters
- Monitoring and reporting of key metrics including:
    - Database availability
    - PostgreSQL service health
    - Database deadlocks
    - Autovacuum
    - Database cluster alive check
    - Connections
    - Storage

Database Service Diagnosis and Troubleshooting

- Diagnosis of database system incidents
- Troubleshoot and work to resolve database system incidents
- Engagement of Microsoft help desk support
- Document user issues and database system errors

PostgreSQL Database Security Management

- User creation and security maintenance
- Database authentication management
- Database encryption management where appropriate

PostgreSQL Database Administration

PostgreSQL database administration is defined as the tasks to maintain the individual databases on the PostgreSQL server.

These tasks include administration and tuning the following areas within the database:

Azure Database for PostgreSQL Single Server:

- Configuration: Management of server-level parameters, such as memory allocation, connection limits, and log retention
- Database Creation: Creating new databases within the PostgreSQL server
- Backup and Restore: Verifying regular backups, performing restores, and ensuring data protection
- Scaling: Adjusting the compute and storage resources of the PostgreSQL server to meet changing workload demands
    - Scaling up Make changes as requested via service ticket submission
    - Scaling down Make changes as requested via service request submission
        - Limited to 1 change per quarter
    - Performance Tuning: Query performance review, index analysis, and standard database maintenance
    - High Availability (where applicable): Configuring replication, failover, and solutions for maintaining high availability and data protection
    - Patching and upgrades (where applicable): Scheduling maintenance period to apply security updates and version upgrades to keep the server environment secure and up to date
        - Version upgrades limited to Flexible Server

Database Cloning

- Cloning/copying/refreshing of databases to a non-production environment for system testing, training, or development.
- Number of clones per database is limited to one (1) per month
- Document applicable database cloning administration procedures

Expert-to-expert helpdesk support

- 24 x 7 technical support for priority 1 and 2 incidents
- 8 am to 5 pm technical support for priority 3, 4 and 5 incidents

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Microsoft Azure Subscription

- Azure subscription and resources needed to support Azure Database for PostgreSQL
- Provide Company access to Azure s subscriptions
- Azure monitoring resources (Azure Monitor, Log Analytics)

Third Party Application Dependency Management

- Management of third-party application interface to the database

Database schema and content management

- Development and/or customization of database schema
- Content management

604670 PostgreSQL Azure PaaS Server Administration - Cores

Company's Responsibilities and Included Features

This PostgreSQL Azure PaaS Server Administration - Cores SKU provides scalable management based upon the number of cores for SKU 604669 PostgreSQL Azure PaaS Server Administration - Base Provide PostgreSQL instance and database administration as documented in ItemID 604669 up to the contracted core count for this ItemID 604670.

Category: Managed End User Support

103057 Helpdesk support per call for remote desktop support and common application support (per call pricing) minimum 20 calls/month set commitment

Company's Responsibilities and Included Features

End-User Support

- An End-User is defined as an individual that has been identified and provided client approval for reporting/escalating incidents/problems to Company
- Event notification receipt by phone, email or web portal
- 24/7 365 days support contact availability
- Tiered technical support environment
- Event Escalation
- Self-Service Web Portal Access
- ITIL approach to event handling Remote User Windows Desktop Support
- Windows 7 or greater
- Remote troubleshooting according to standards for operating systems
- Remote troubleshooting of applications is limited to common applications such as MS Office applications (Word, Excel, PowerPoint, Outlook), Acrobat Reader, Internet Explorer
- Remotely re-install software that is a common application to resolve an issue (not including file read compatibility issues).

Software must be available on a LAN local to the user
    - Install driver, verify connectivity and print test page according to standards for client approved LAN printers available from Active Directory via a Print Server
- Remote troubleshooting of connectivity to client corporate wired or wireless network at a client corporate location
- Virus remediation is limited to use of antivirus software available on the workstation

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hardware and software purchasing and licensing and deployment

- Procurement of OS and application software and licensing for current version on current operating system, including any user or processor access licensing
- Procurement of current software support and maintenance where applicable
- Procurement of hardware
- All shipping charges
- Deployment of software to existing and new users
- Imaging and deployment of systems to existing and new users (including setup and configuration of the user on a system) Non-Supported Issues
- Repairing corrupted Office files (including Company)
- Deployment/Installation of software or software upgrades
- Support of desktop peripherals
- Installation of driver software for peripherals such as scanners, external storage devices and input devices, including internal mobile Wi-Fi cards
- VPN connectivity support is not included unless provided as part of another Company service
- Management and maintenance of antivirus and antimalware applications and console is not included unless provided as part of a Company service
- Operating system patching is not included unless provided as part of another Company service
- Application patching is not included
- Support of non-domain network connectivity is not included (this includes public Wi-Fi, mobile hotspots and home Wi-Fi)
- Group policy management backup infrastructure and management*
- Provide backup system, infrastructure or service
- Manage desktop backups
- *Unless provided through Company managed VDI, Citrix or RDS Environment Requirements
- Supported systems must be a member of a single domain
- Systems must have IP address allocated via DHCP scope
- Company may run periodic inventory scans on the network to validate count of supported systems

103057-N Helpdesk support per call for remote desktop support and common application support (per call pricing) minimum 20 calls/month set commitment

Helpdesk support per call for remote desktop support and common application support (per call pricing) minimum 20 calls/month set commitment

301492 End User Service Desk Services

Company's Responsibilities and Included Features

General

Company shall provide a service desk for receipt of tickets.

- The service desk shall be available 24 x 7 x 365
- All new Tickets will be received via the Company service desk email or phone number. The technician will create an incident in the Company incident management system along with a number which is used to keep track of the status and work completed for the ticket. Following receipt of the ticket, the service desk will triage the incident and resolve the incident if the Client has provided Company with a pre-provided detailed triage and troubleshooting instructions, otherwise the Incident will be escalated to a second level support resource within the Client organization, third party support vendors or within Company if Company is contracted to provide that level of support.
- Client shall collect and provide a reasonable level of detail to the Companies service desk to enable effective triage and escalation of the ticket.
- When Company believes that the ticket has been escalated to resources outside of Company, resolved or fulfilled, documentation of the activities performed will be updated in the incident record and the incident record will be set to a resolved status.
- Service is limited to 300 support tickets per month
- Incidents that require greater than 15 minutes of effort will be escalated to second level support resources.
- Company will provide a dedicated toll-free phone number for users to call the service desk.

Service Desk Service Criteria

Service Level	Service Target
Call wait time	Less than 1 minute for 95% of tickets
Email response time	Less than 60 minutes for 95% of tickets
Resolution or escalation of Ticket	Within 20 minutes from the time the ticket is responded to for 95% of tickets.

Ticket Reporting

Company will provide periodic reports on ticket statistics and metrics

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Triage, Troubleshooting and Escalation Procedures

Documentation providing detail instructions as to:

- How the Companies service desk should triage and troubleshooting an incident
- When, what and how to escalate incidents to 2nd level support organizations

500052 Desktop Virus Control (powered by Lumension) - 20 seat minimum

Company's Responsibilities and Included Features

Centralized virus control for desktops associated with a managed IT environment includes:

- AV software licensing, maintenance and support
- Removal of existing legacy virus control software (if applicable)
- Automatic virus control pattern file updates
- Virus trending and compliance reporting
- Client software install point made available to Client IT personnel for desktop roll-out
- Virus outbreak containment and management including priority alerts to client contacts
- Automated roll-out of AV software and updates

Advanced system administration support for AV software

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Logical access presented to Company for desktops/laptops to be covered with AV Remote hands for desk-side support issues related to implementation and management
- Virus control for inbound corporate email
- End user support for all applications and components other than AV software components

600476 Help Desk and User Support

Company's Responsibilities and Included Features

This service is provided by a third-party service provider, the Bross Group (Provider) and contracted through the Company.

Help Desk and User Support

- User support is provided to Client users related to the operation of Client provided Personal Computers (PC or PCs).
- Troubleshoot and maintain operating systems, apply updates, load authorized applications, setup and provision replacement PCs.
- Providers Help Desk will assist in ensuring applications load on a user's PC.
- User support requests can be made via email to the provider support portal, by logging into the support portal and creating a support request.
- User support is provided for up to 50 Client users and PCs
- An additional monthly service fee will added for every PC added to environment above fifty (50) PCs. See ItemID 600477-Additional PC Monitoring - over 50 PCs
- Provider is responsible for ongoing maintenance, of Client provided PCs to include:
    - Troubleshooting and resolution of issues
    - Routine patching
    - Installation of authorized software
    - Warranty repair facilitation
    - User access management
    - Operating System updates
    - PC setup
- Help Desk and User Support is limited to forty (40) hours of support per month
    - If more hours are needed in any month the Client may:
        - Purchase additional hours
        - Defer requested work to the following month
        - Borrow hours from the next month
    - Client can roll over one calendar quarters worth of hours into the following quarter
        - Rollover hours can be used for IT functions at the Clients request
    - Client is charged for the actual time used for a given ticket
        - Time is tracked within the ticketing software
    - Travel time to remote locations, outside of Denver metro area, consumes support hours
    - Current month hours are consumed before unused hours
    - Unused hours can roll over from a single month to the next month
    - Provider will provide Client with a monthly report of used, unused and carried over hours
    - Provider will report on support usage in 10-hour increments to the Client
- Antivirus.
    - Install and maintain Client purchased and approved antivirus package on PCs. When possible, will deploy the package from a central server location to all in scope client endpoints. Includes the reporting and alerting to client on any incidents.
- PC Monitoring / Alerting.
    - Provider will provide and use an enterprise class monitoring system to monitor all PCs under the scope of the managed services contract.

        - All monitors will be configured with thresholds and boundaries approved by the Client
        - Actions, incidents or performance outside of approved boundaries or thresholds will trigger an automatic alert to the Provider support team.
- Reporting
    - Usage statistics
    - Inventory
    - Routine performance reporting of all systems
- Internal network device management
    - Maintenance of wireless access points
    - All hardware must be covered by a End Client procured maintenance contract for support
    - Cabling and cable jacks are not in scope of the managed services contract
    - Hardware replacement will fall under a time and material project
- Asset tracking
    - Deployment of monitoring and tracking agent to all covered systems, to provide health and basic statistics of the deployed device or server
- General IT advisory services
    - Provide general IT input and advice
- Provider End User Support Portal
    - Tracks and provides reporting support for all Client work for in scope systems.
    - Client may submit work or change requests via the online portal or email.
    - An online knowledgebase is available in the portal to assist users with article to resolve issues without technician support.
    - Support time will be entered and tracked in this system.
- Coverage
    - Normal Business Hours - Monday to Friday 8:00 am to 5:00 pm MST time. Support will primarily be performed remotely.
    - Onsite support will be provided as needed, although not typically expected to exceed one visit per month.
    - Support provided outside of these hours will be charged per hour at the rate contracted under Item Id 600478
- Maintenance Windows
    - Maintenance Windows are pre-scheduled times where the support team will perform required or routine maintenance activities as described above.
    - These windows will have a designated start time and a target end time and are generally scheduled after normal business hours.
    - Client will be notified when the window begins and ends.
    - Client systems may not be available during these maintenance windows.
    - In scope services conducted during Maintenance Windows that are outside normal business hours are considered normal support and do not incur additional after hours charges.
    - Scheduling notifications will be provided in advance, typically no later than two weeks previous to the planned Maintenance Window.
    - Provider reserves the right to perform critical or emergency maintenance with no notice. In these instances, every attempt will be made to provide as much notice as possible and to avoid Normal Business hours.
- Hardware Support
    - All hardware supported as part of the End Client environment must be on a current warranty or support contract. Provider will facilitate troubleshooting and maintenance with the support vendor and facilitate warranty replacement for failing hardware under this agreement
- Provider will provide support for any out of scope items upon mutual agreement by Client and provider. All out of scope support provided will consume support hours.

Support Levels

The following describes the Provider support levels for user support:

Support Level	**Description**
Level 1	All support incidents begin in Level 1 Support, where the initial trouble ticket is created, the issue is identified, and

Support	clearly documented, and basic hardware/software troubleshooting is initiated.
Level 2 Support	All support incidents that cannot be resolved with Level 1 Support are escalated to Level 2 Support, where more complex support on hardware/software issues can be provided by more experienced engineers within Provider.
Level 3 Support	Support Incidents that cannot be resolved by Level 2 Support are escalated to Level 3 Support, where support is provided by the most qualified and experienced engineers within Provider who have the ability to collaborate with 3rd party vendor support engineers to resolve the most complex issues.

Response and Resolution Times

The following table shows the targets of response and resolution times for each priority level.

Priority	Trouble	Response Time (hours)	Resolution Time (hours)	Escalation Threshold (hours)
1	Service not available (all users and functions unavailable).	Within one (1) hour, Normal Business hours	ASAP - Best Effort	2
2	Significant degradation of service (large number of users or business critical functions affected)	Within four (4) hour, Normal Business hours	ASAP - Best Effort	8
3	Limited degradation of service (limited number of users or functions affected, business process can continue).	Within 24 hour, Normal Business hours	ASAP - Best Effort	48
4	Small service degradation (business process can continue, one user affected).	Within 48 hour, Normal Business hours	ASAP - Best Effort	96

Service Request Escalation Procedure

Support Request Initiation:

1. Support request is received
    - Preferred email is sent to support first
    - If email is not functioning ticket is opened in support portal
    - Critical issue email is sent to support first, then a phone call is made to support to escalate the issue
2. Trouble ticket is created
3. Issue is Identified and documented in service request system
4. Issue is qualified to determine if it is an issue to be escalated to Company or if it can be resolved through Level 1 Support

If issue is be escalated to Company:

1. Level 1 resolution - Issue is escalated to Company
2. Trouble Ticket is closed in Providers service request system

If issue can be resolved through Level 1 Support:

1. Level 1 resolution - Issue is worked to successful resolution
2. Quality control - Issue is verified to be resolved to Clients satisfaction
3. Trouble Ticket is closed, after complete problem resolution details have been updated in service request system

If issue cannot be resolved through Level 1 Support:

1. Issue is escalated to Level 2 Support
2. Issue is qualified to determine if it can be resolved by Level 2 Support

If issue cannot be resolved through Level 1 Support:

1. Issue is escalated to Level 2 Support

2. Issue is qualified to determine if it can be resolved by Level 2 Support

If issue can be resolved through Level 2 Support:

1. Level 2 resolution - Issue is worked to successful resolution
2. Quality control - Issue is verified to be resolved to Clients satisfaction
3. Trouble Ticket is closed, after complete problem resolution details have been updated in service request system

If issue cannot be resolved through Level 2 Support:

1. Issue is escalated to Level 3 Support
2. Issue is qualified to determine if it can be resolved through Level 3 Support

If issue can be resolved through Level 3 Support:

1. Level 3 resolution - Issue is worked to successful resolution
2. Quality control - Issue is verified to be resolved to Client's satisfaction
3. Trouble Ticket is closed, after complete problem resolution details have been updated in service request system

If issue cannot be resolved through Level 3 Support:

1. Issue is qualified to determine if it can be resolved through sending a support engineer onsite
2. An onsite visit will be scheduled if appropriate
3. Onsite resolution - Issue is worked to successful resolution
4. Quality control - Issue is verified to be resolved to Client's satisfaction
5. Trouble Ticket is closed, after complete problem resolution details have been updated in service request system

If issue can be resolved through Onsite Support:

1. Onsite resolution - Issue is worked to successful resolution
2. Quality control - Issue is verified to be resolved to Clients satisfaction
3. Trouble Ticket is closed, after complete problem resolution details have been updated in service request system

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Out of Scope Notes

- Application support is defined as support designed to help a user use the feature and function sets of an application, such as Excel, PowerPoint, etc. Application support is not provided.
- Infrastructure system upgrades is out of scope Due to the complexity and potential dependencies between applications, upgrades to a server operating system, a database version or an application upgrade can only be performed as part of a separately authorized and funded project. These activities will be performed under a separate Statement of Work (SOW) or under the block of hours support outlined in this agreement, if available.
- Replacement of infrastructure hardware is not included as part of this agreement. Infrastructure hardware replacement will be performed as part of a separate SOW or under the contracted block of hours support outlined in this agreement, if available.
- Acquisition of hardware is the Client's responsibility. Provider will facilitate and participate in the selection as desired. Provider will make recommendations for personal computer hardware replacement cycle for the client's review and approval.
- Any item not specifically noted as in scope is considered out of scope
- Virtual desktop support, maintenance and monitoring is out of scope
- Security system maintenance and support is out of scope
- Printer hardware maintenance and support are out of scope
- Microsoft Remote Desktop Services support is out of scope

Client responsibilities

- User support requests can be made via email, customer portal or by phone.

        - Email is the required means to create a ticket with the helpdesk, whether the issue is critical in nature or not
        - User support requests can also be created in the customer portal if email is not functioning properly
        - For critical issues it is required that a ticket is opened by emailing the issue to the helpdesk and then calling in for support to escalate the ticket
    - Client is responsible to contribute to the success of the Maintenance Windows by participating in planning and scheduling of appropriate pre-maintenance activities and to perform post maintenance testing and acceptance of the planned changes.

600477 Additional PC Monitoring - over 50 PCs

Company's Responsibilities and Included Features

This service is provided as an add on to item 600476-Help Desk and User Support and provides monitoring of additional PCs over and above the 50 PCs included under 600476-Help Desk and User Support.

Item 600476-Help Desk and User Support is required for this service.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

None

600478 After Hours Support and Overages

Company's Responsibilities and Included Features

- This service is provided as an add on to item 600476-Help Desk and User Support and defines the rate for providing Help Desk and User Support outside Normal Business Hours as defined in item 600476-Help Desk and User Support or providing Help Desk and User Support over the contracted monthly bucket of hours for item 600476-Help Desk and User Support.
- Provider will obtain approval from Client to conduct Help Desk and User Support outside Normal Business Hours or in excess of contracted bucket of hours. This will be billed on a metered basis, as tracked by Provider.
- After hours support can leverage the monthly hours associated with item 600476. Hours consumed after hours would decrement the monthly hours associated with item 600476 at an accelerated rate of 1:1.65.
- Item 600476-Help Desk and User Support is required for this service.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

601396 End User Service Desk Support

Company's Responsibilities and Included Features

Service Desk

- Company shall provide a service desk for receipt, triage and first level resolution or escalation of Client's end user tickets.
- All new tickets will be received by the Company service desk either through a Client's user entering request or incident into the Client's incident management system. For phone initiated tickets, the Company technician will create an Incident in the Client's incident management system. Following receipt of the ticket, the Company service desk will triage the incident and resolve the incident if the Client has pre-provided detailed triage and troubleshooting instructions, otherwise the ticket will be escalated to a second level support resource within the Client organization, third-party support vendors or within Company if Company is contracted to provide that level of support.
- Company will not receive any emails or phone calls through the Company s main service desk. Email tickets will appear in a queue in the Client s ticketing system and phone calls are to be routed through a special vanity number
- When Company believes that the ticket has been escalated to resources outside of Company, resolved or fulfilled,

documentation of the activities performed will be updated in the Incident record and the Incident record will be set to a Resolved status.
- Incidents that require greater than 30 minutes of effort will be escalated to second level support resources.
- Company will provide a dedicated toll-free phone number for users to call the service desk.
- This service is limited to the contracted ticket quantity. Tickets usage will be based upon the date the ticket was created. Monthly ticket usage will be calculated as a three-month rolling average.

Service Desk Hours

The Company Service Desk shall be available during the following hours.

- Monday to Friday - 5:00pm to 9:00am CDT
- Weekends - up to 12:00 am CDT
- Bank holidays - up to 12:00 am CDT

Service Desk Service Criteria

Company strives to respond to your support request in a timely fashion. The following outlines the service level targets.

Service Level	Target
Call wait time	Less than 1 minute for 95% of Tickets
Email response time	Less than 60 minutes for 95% of Tickets
Resolution or escalation of Ticket	Within 20 minutes from the time the Ticket is responded to for 95% of Tickets.

Ticket Reporting

Company will provide periodic reports on ticket statistics and metrics

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Incident Management System

- Provide Company technicians access to Client provided and managed incident management system
- Provide necessary incident management system user licensing for Company technicians

- Provide the access/ability for Company to download service ticket metrics including, the number of tickets handled and the time spent on each ticket for our own reporting purposes, both for billing and for service desk performance metrics.

Triage, Troubleshooting and Escalation Procedures

Documentation providing detail instructions as to:

- How the Companies service desk should triage, troubleshooting and/or resolve a ticket
- When, what and how to escalate incidents to second level support organizations
- When, what and how to defer incidents to NBD and the Client's help desk
- All documentation (including on-call name/schedule) to be provided in such a manner to allow Company to store their own copies.

Client to provide Company with training and orientation similar to that of their new hire process.

- Shadows Client help desk employee working through calls and tickets, then roles are reversed, and Company Agent is now working tickets/calls with assistance from tenured Client help desk individual.

Incident Reporting

- All new tickets are to be initiated either through a Client's user entering request or incident into the Client's incident management system or via the Client's main help desk email or phone number
- Client shall collect and provide a reasonable level of detail to the service desk to enable effective triage and escalation of the ticket.
- If Client becomes aware of any additional information regarding the ticket, Client shall use reasonable efforts to provide this information to Company in a timely manner.

601462

Company's Responsibilities and Included Features

Service Desk

- Company shall provide a service desk for the receipt, triage and first-level resolution or escalation of Client's end-user tickets
- All new tickets will be received by the Company service desk either through a Client's user calling the Client s service desk phone number which will be routed to Company, or by entering a request or incident into the Client's incident management system. For phone initiated tickets, the Company technician will create an incident in the Client's incident management system. Following receipt of the ticket, the Company service desk will triage the incident and work to resolve the incident if Client has pre-provided detailed triage and troubleshooting instructions, otherwise the ticket will be escalated to a second level support resource within the Client organization, third-party support vendors or within Company if Company is contracted to provide that level of support.
- Phone calls are to be routed from Client through a special vanity number provided by Company.

Ticket Volume

- This service is limited to up to 150 calls per day.
- If the volume of calls is exceeding 150 calls per day, upon notice by Company, Client agrees to meet with Company to address the overage by reducing call volume or entering into a change order as mutually agreed by the parties.

.

Service Desk Hours

- The Company Service Desk shall be available Monday to Friday - 7:00am to 5:00pm CDT/CST

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Incident Management System

- Provide Company technicians access to Client provided and managed incident management system
- Provide necessary incident management system user licensing for Company technicians
- Provide the access/ability for Company to download service ticket metrics including the number of tickets handled and the time spent on each ticket for Company s reporting purposes, both for billing and for service desk performance metrics.
- Company may need to have up to 10 Company technicians logged into the Client s service desk environment at any one time. System resources must be adequate to provide reasonable performance.

Triage, Troubleshooting and Escalation Procedures

Documentation providing detail instructions as to:

- How the Company's service desk should triage, troubleshooting and/or resolve a ticket
- When, what and how to escalate incidents to Client second level support organizations including Client's Major Incident Manager (MIM)

Incident Reporting

- All new tickets are to be initiated either through a Client's user entering request or incident into the Client's incident management system or via the Client's main help desk email or phone number
- Client shall collect and provide a reasonable level of detail to the service desk to enable effective triage and escalation of the ticket.
- If Client becomes aware of any additional information regarding the ticket, Client shall use reasonable efforts to provide this information to Company in a timely manner.

601519

Company's Responsibilities and Included Features

Service Desk

- Company shall provide a service desk (Service Desk) for after-hours receipt, triage and first level response to Client's end users ticket requests.
- All after-hour incidents will be received by the Service Desk via phone initiated service tickets only. Following receipt of a phone initiated service ticket the Company technician will create an incident in the Client's incident management system. The Service Desk will triage and attempt to resolve the incident if the Client has pre-provided detailed triage and troubleshooting instructions, otherwise, the ticket will be escalated to a second level support resource within the Client organization, third-party support vendors or within Company if that level of support is included in Client s contracted scope of services with Company.
- Client example of support items:
  - Password changes
  - Password resets
  - Local user printer setup
- Company will not receive any phone calls directly to the Company s main service desk. Phone calls are to be routed by the Client from the Client s main help desk phone number to a special vanity number provided by Company.
- When Company believes that the ticket has been escalated to resources outside of Company, resolved or fulfilled, documentation of the activities performed will be updated in the Incident record and the Incident record will be set to a Resolved status.
- Company will provide a dedicated toll-free phone number for users to call the Service Desk.
- This service is limited to the contracted ticket quantity. Tickets usage will be based upon the date the ticket was created. Monthly ticket usage will be calculated as a three-month rolling average.
- The Company to follow the Client s escalation protocol for these applications:
  - CRM
  - Sapphire

After Hours Service Desk

- Monday to Friday - 5:00pm EST to 9:00am EST
- Weekends - from Friday 5:00pm EST to Monday 8:00am EST
- The following holidays:- 12:00am to 11:59pm EST
  - New Year s Day
  - Christmas Day
  - Memorial Day
  - 4th of July
  - Labor Day
  - Thanksgiving Day

Service Desk Service Criteria

Company strives to respond to your support request in a timely fashion. The service level target for call wait time is less than one (1) minute for 95% of ticket requests.

Ticket Reporting

Company will provide periodic reports on such ticket statistics and metrics as mutually agreed to by Company and Client.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Incident Management System

- Provide incident management system managed by Client.
- Provide Company technicians access to Client incident management system.
- Provide necessary incident management system user licensing for Company technicians.
- Provide the access/ability for Company to download service ticket metrics from Client s incident management system, including but not limited to the number of tickets handled by Company and the time spent on each ticket.

Triage, Troubleshooting and Escalation Procedures

Documentation providing detailed written instructions as to:

- How the Service Desk should triage, troubleshoot and/or resolve tickets.
- When, what and how to escalate incidents to second level support at Client (including contact information and associated schedules) or with third parties.
- When, what and how to defer to Client's help desk.
- All required documentation to be provided in such a manner to allow Company to store copies of such documentation.

Training and Orientation

Client to provide Company with training and orientation related to help desk support. As part of this training and orientation Company technicians will shadow Client help desk employee working through calls and tickets, then Company technician will work calls and tickets with assistance from tenured Client help desk individual.

Incident Reporting

- All new tickets are to be initiated via the Client's main help desk phone number.
- Client shall collect and provide a reasonable level of detail to the service desk to enable effective triage and escalation of the ticket.
- If Client becomes aware of any additional information regarding the ticket, Client shall use reasonable efforts to provide this information to Company in a timely manner.

601723 Staff Augmentation Service

Company's Responsibilities and Included Features

Company shall provide a named resource (Resource) for the purpose of providing information technology (IT) staff augmentation services. The Resource will provide Services for the upkeep, configuration, and operation of servers and back-office IT infrastructure as well as end-user compute technical support, all at the direction and request of Client.

Staff Augmentation Service

Company shall provide up to 128 total hours per month of staff augmentation Services using a combination of remote and on-site assistance.

- Up to 96 hours of on-site support, with the remaining hours to be performed remotely
- Remote staff augmentation services may be delivered using any combination of the following methods:
  - Telephone
  - Web video/audio conferencing
  - Remote control software
- Unless otherwise agreed to by Company, on-site work shall be performed at the following Client location: LifeServe Blood Center, 431 E Locust Street, Des Moines, IA 50309
- Staff Augmentation is to be performed during regular business hours: Monday through Friday, 8:00 am to 5:00 pm, Client's local time zone and excluding holidays recognized by Company
- Company and Client will mutually determine an on-site schedule
- Company may use additional resources in the event the Resource is unavailable

- Unused hours are forfeited and are not rolled over or banked into the following month. No credit shall be provided for unused hours.

This service is separate from the managed Services provided to Client under this SOW.

Service Level Agreement

Service Level Agreements (SLA) as provided in this SOW do not apply to this Service.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General

- Overall responsibility for the design, desired performance, and operations of servers and back-office IT infrastructure.
- Overall security of Client desktops, servers, applications, operating systems, and back-office IT infrastructure.
- IT hardware and software and associated maintenance and / or support contracts.

Incident Management System

- Provide Company Resource with access to Client s IT service management software/incident management system
- Provide the Company Resource with physical access to Client site and IT infrastructure

Support Requests

Client shall comply with Company's standards for support and services requests as defined within the Company s Customer Operations Handbook including, but not limited to, making requests through Company's Service Desk system. Support requests can be created electronically by sending e-mail to servicedesk@oneneck.com.

602352 Managed Windows Desktop Patching

Company's Responsibilities and Included Features

Company will provide Windows operating system patching for Client s Personal Computers (PCs) such as workstations, desktops, and laptops running Microsoft Windows 10 Operating System (OS) as follows:

Windows PC Patch Management

- Weekly reviews of Microsoft published critical patches for OS
- Weekly scheduled application of patches during Client approved patch windows
- Client can request additional patch windows up to 1 patch window per 200 PCs per monthly patch cycle
- Patch management will be provided through a Company licensed and managed centralized patching solution
- Patching of PCs occurs over the internet through port 52311
- Provide patch management compliance reporting on an ad hoc basis or as part of the monthly patch cycle
- Patching cycle occurs once a month
- Patch process cycle occurs over a 2-week period each month with the following primary steps.
    - Analyze patches needed and provide Client with a report
    - Push patches to a test/dev PC Group
    - Re-analyze test/dev PC Group patches and provide Client with a report
    - Push patches to covered PCs during Client approved patch window/s
    - PC reboots may be required of Client end users after patch application

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Windows PC Patch Management

- Approve patching windows as requested by Company

End User, Hardware and Operating System Support

- Remote hands for desk-side support issues related to patch management
- Requires minimum OS of Windows 10
- All backups of PCs
- End user hardware and operating system support
- Windows OS version upgrades
- Support of all applications and components loaded onto the PC other than Company provided patch agents
- Ensure all PCs to be patched by Company are accessible over the internet through port 52311
- Follow up on PCs that failed to patch or which were unavailable to patch during patching window
    - Company will provide Client with a list of applicable PCs
    - Client is responsible for resolving any issues preventing patching
- Rollback/uninstall of patches and inform Company of any rollback/uninstall of patches

Operating System Licensing and Antivirus Protection

- Procure OS software licensing
- Procure and manage PC antivirus protection

Application Patching

- Patch all applications on the PC
- Patch and update the antivirus system

Patch Testing

- Identify and provide a list of PCs to Company that will be used as the single patch test group that are representative of the total group of PCs to be patched (a test/dev PC Group)
- Review and approval to patch based upon patch reports provided by Company
- Test the test group of PCs after monthly test patching has been applied within the agreed-upon time window. Remaining PCs will not be patched by Company until Client confirms to Company that testing is complete and patching may commence.
- Client to inform Company of patches that should not be applied.

611128 Custom After-hours Service Desk Support

Company's Responsibilities and Included Features

Company's Responsibilities and Included Features

Providing after hours help desk services to triage, escalate and resolve where Client has provided the necessary knowledge articles.

Company will respond to incidents and service requests initiated via:

- Client-initiated transference of voice system calls
- Service Request tickets on Company s ITSM system opened via email from Client s email system

After Hours Support Hours

Company will provide help desk services during the following times (all times are Central Time):

- 5:00PM to 7:00AM weekdays
- 5:00PM Friday evening to 7:00AM Monday morning
- The following holidays, beginning at 5:00PM from the preceding regular workday and returning to service at 7:00AM the following workday:
    - New Year s Day
    - Martin Luther King Day
    - President s Day
    - Memorial Day

- Juneteenth
- Independence Day
- Labor Day
- Veteran s Day
- Thanksgiving
- Day-after Thanksgiving
- Christmas Day

Help Desk Services

- Provide password reset initiation service to end-user callers.
- Provide basic Windows desktop and equipment troubleshooting assistance to end-user callers.
- Escalate/transfer to Client s help desk for next-business-day support for matters that cannot be immediately resolved as documented by Client in knowledge articles.
- Respond to incidents consistent with Client s support escalation procedures and knowledge articles.
- Escalate, as necessary, to Client s on-call staff as described in Client s procedure manuals or knowledge articles.
- Provide systems incident response service for up to 150 applications, 400 network devices and 500 servers.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Initiate forwarding and un-forwarding of help desk calls to Company at the designated times.
- Facilitate Company s access to Client s monitoring and alerting applications.
- Configure and maintain a mailbox on Client s email system that is tied to Client s IT monitoring and alerting system and sends emails to Company s service desk email address.
- Facilitate access to and maintain support escalation procedure manual and knowledge articles.
- Ensure availability of monitoring and alerting applications and email box used for the service.

Category: Managed Networks

100092 Wireless Access Point Management (lightweight)

Company's Responsibilities and Included Features

Autonomously managed Wireless Access Point

- Proactive monitoring
- Device configuration
- Facilitate upgrades

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hardware Maintenance Coverage

- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that Company is an authorized caller to maintenance service providers End User Wireless Support
- End User device wireless support

100093 Wireless Access Point Management (autonomous)

Company's Responsibilities and Included Features

WAP Management Autonomously managed Wireless Access Point

Proactive monitoring

- Device configuration
- Facilitate upgrades

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hardware Maintenance Coverage

- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that Company is an authorized caller to maintenance service providers End User Wireless Support
- End User device wireless support

100098 Network Load Balancer Appliance Management

Company's Responsibilities and Included Features

Maintain Application Rules with configuration of up to 20 unique application flows:

- Load balanced IP
- SSL Certificate management
- Real server configuration
- Pattern match rules
- Redirect rules

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hardware Maintenance Coverage

- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Ensure that Company is an authorized caller to maintenance service providers

100292 Dedicated Basic Router Management

Company's Responsibilities and Included Features

Router Management (Basic)

- Management of interface IP addresses
- Configuration of basic routing (Static, RIP, (E)IGRP, single-are OSPF, etc.)
- IP interface availability monitoring and performance reporting
- NTP service management if needed
- Circuit Management (Single circuit per device)
- Monitor circuit for up/down status
- Report on circuit bandwidth utilization via monitoring on managed router
- Error and discard reporting
- Identify outages and escalate to circuit vendor by opening trouble ticket
- Escalate trouble tickets with vendor following Company standard operating procedure
- Requires LOA with carrier to open tickets on client s behalf

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hardware Maintenance Coverage

- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that Company is an authorized caller to maintenance service providers Remote Hardware Support
- Provide remote hands-on support if physical intervention is required for troubleshooting

Hardware Maintenance Coverage
- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Ensure that Company is an authorized caller to maintenance service providers

Remote Hardware Support
-Provide remote hands-on support if physical intervention is required for troubleshooting

100293 Dedicated Advanced Router Management

Company's Responsibilities and Included Features

Router Management (Advanced)

- Management of interface IP addresses
- Configuration of routing protocols (Static, RIP, EIGRP, OSPF, etc.)
- IP interface availability monitoring and performance reporting
- NTP service management if needed Site-to-site VPN Management
- Management of the VPN Tunnel configurations on one side of a Point-to-Point VPN connection
- Management of the DMVPN Tunnel configurations for NHRP on one side of the endpoint mapping
- Troubleshooting/support of VPN/DMVPN tunnel establishment Circuit Management (Single circuit per device)
- Monitor circuit for up/down status
- Report on circuit bandwidth utilization via monitoring on managed router
- Error and discard reporting
- Identify outages and escalate to circuit vendor by opening trouble ticket
- Escalate trouble tickets with vendor following Company standard operating procedure
- Requires LOA with carrier to open tickets on client s behalf

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hardware Maintenance Coverage

- Procurement of hardware maintenance for the duration of this Statement of Work
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that Company is an authorized caller to maintenance service providers Client-side VPN Termination Device For a Point to Point VPN tunnel, the Client will be required to provide and configure a Client side VPN termination device and internet connectivity with the following attributes:
    - IPSec capable device
    - Static public IP address Remote Hardware Support

- Provide remote hands-on support if physical intervention is required for troubleshooting

Hardware Maintenance Coverage
- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that OneNeck is an authorized caller to maintenance service providers
Client Side VPN Termination Device

For a Point to Point VPN tunnel, the customer will be required to provide and configure a customer side VPN termination device and internet connectivity with the following attributes:
- IPSec capable device
- Static public IP address
Remote Hardware Support
-Provide remote hands-on support if physical intervention is required for troubleshooting

100295 Dedicated Layer-2 Switch Management (up to 48 ports)

Company's Responsibilities and Included Features

Layer 2 Management

- Spanning tree configuration
- VLAN Assignment
- Port Assignment
- Etherchannel configuration and management
- 802.1Q VLAN Trunk configuration and management

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hardware Maintenance Coverage

- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that Company is an authorized caller to maintenance service providers

Hardware Maintenance Coverage
- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that OneNeck is an authorized caller to maintenance service providers

100297 Dedicated Layer-3 Switch Management w/ Basic Routing (up to 48 ports)

Company's Responsibilities and Included Features

Layer 2 Management

- Spanning tree configuration
- VLAN Assignment
- Port Assignment
- Etherchannel configuration and management
- 802.1Q VLAN Trunk configuration and management Layer 3 Management (Basic)
- Management of interface IP addresses
- Configuration of basic routing (Static, RIP, (E)IGRP, single-are OSPF, etc.)
- IP interface availability monitoring and performance reporting
- NTP service management if needed

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hardware Maintenance Coverage

- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that Company is an authorized caller to maintenance service providers

Hardware Maintenance Coverage
- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that OneNeck is an authorized caller to maintenance service providers

103042-N Managed Basic Router Setup

Company's Responsibilities and Included Features

- Receive, Unpack and Install Device in Rack
- Cabling (power, network)
- IOS updates (If applicable)
- Configure Interfaces/routing/ACL
- Documentation updates (portal, tasks, support center)
- Configure and verify backups and monitoring (If applicable)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

103043-N Managed Advanced Router Setup

Company's Responsibilities and Included Features

- Receive, unpack and install device in rack
- Cabling (power, network)
- IOS updates (If applicable)
- Configure Interfaces/routing/ACL
- Documentation updates (portal, tasks, support center)
- Configure and verify backups and monitoring (If applicable)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

103044-N Managed Layer-2 Switch Setup

Company's Responsibilities and Included Features

- Receive, unpack and install device in rack
- Cabling (power, network)
- IOS updates (If applicable)
- Configure Interfaces/routing/ACL
- Documentation updates (portal, tasks, support center)
- Configure and verify backups and monitoring (If applicable)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

103045-N Managed Layer-3 Switch w/ Basic Routing Setup

Company's Responsibilities and Included Features

- Receive, unpack and install device in rack
- Cabling (power, network)
- IOS updates (If applicable)
- Configure ports/VANS/SVIs/routing
- Documentation updates (portal, tasks, support center)
- Configure and verify backups and monitoring (If applicable)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

103047 Network Monitoring Only (per Network device)

Company's Responsibilities and Included Features

Monitoring

- Hardware Port (when Applicable)
- System Performance thresholds
- Critical Services
- Non-security event log monitoring
- Basic ICMP Monitoring

Notification

- Notification via e-mail of priority incidents

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide read SNMP access
- Have associated firewall ports open to allow for monitoring traffic

103407-N Network Monitoring Only (per Network device)

Company's Responsibilities and Included Features

- Deploy and configure monitoring of network device using Company standard template
- Supported technologies: All network devices supported under Company managed services
- Configure monitoring of:

- CPU, memory thresholds (where available)
- Port errors and packet loss (where available)
- Link state for identified critical connections (where available)
- Available hardware threshold: fans status, power supply, temperature (where available)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Resolve issues identified by Company monitoring
- Provide appropriate escalation path for alerts
- Work with Company to adjust and tune alerting thresholds
- Provide appropriate credentials to enable monitoring
- Configure network and devices to meet monitoring requirements

500056 Meraki Cloud Management

Company's Responsibilities and Included Features

Centralized Meraki Cloud Management

- Provide Client access to Meraki dashboard and tools
- Integration of Meraki cloud with the Company monitoring infrastructure
- Monitor and troubleshoot Meraki cloud
- Configuration management of Meraki cloud Centralized Meraki Cloud Operations
- Configure access points using features and capabilities of the controller.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Initial deployment and configurations
- Device must be fully operational so that remote management capability can be configured
- Vendor hardware/software support contract or coverage required for support escalation and updates
- Ensure Company is an authorized caller associated with the vendor support contract
- Ensure Company is provided with vendor support contract contact information
- Client must provide the physical space, power, cabling, console connectivity, etc
- Client must provide remote personnel and access for activities requiring physical presence
- End-user wireless support
- Mobile device management (MDM) support

500058 Meraki Access Point Management: (requires Meraki Cloud Management)

Company's Responsibilities and Included Features

- Configure, monitor, and troubleshoot access points
- Manage replacement and/or repair with support vendor
- Monitor and troubleshoot access points using features and capabilities of the controller and integration with Company monitoring infrastructure
- Update/patch access points using features and capabilities of the controller
- Configuration management of Meraki access point

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Initial deployment and configurations
- Device must be fully operational so that remote management capability can be configured
- Vendor hardware/software support contract or coverage required for support escalation and updates

- Ensure Company is an authorized caller associated with the vendor support contract
- Ensure Company is provided with vendor support contract contact information
- Client must provide the physical space, power, cabling, console connectivity, etc
- Client must provide remote personnel and access for activities requiring physical presence
- End-user wireless support
- Mobile device management (MDM) support

500059 Meraki Primary Switch Management

Company's Responsibilities and Included Features

Meraki Layer 2 Switch Management

- Spanning tree configuration
- VLAN Assignment
- Port Assignment
- Etherchannel configuration and management
- 802.1Q VLAN Trunk configuration and management
- Monitor and troubleshoot switch
- Update/patch switch
- Manage replacement and/or repair with support vendor

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Initial deployment and configurations
- Device must be fully operational so that remote management capability can be configured
- Vendor hardware/software support contract or coverage required for support escalation and updates
- Ensure Company is an authorized caller associated with the vendor support contract
- Ensure Company is provided with vendor support contract contact information
- Client must provide the physical space, power, cabling, console connectivity, etc
- Client must provide remote personnel and access for activities requiring physical presence

500060 Meraki Stacked Switch Management (requires Meraki Primary Switch Management)

Company's Responsibilities and Included Features

Meraki Layer 2 Switch Management

- Spanning tree configuration
- VLAN Assignment
- Port Assignment
- Etherchannel configuration and management
- 802.1Q VLAN Trunk configuration and management
- Monitor and troubleshoot switch
- Update/patch switch
- Manage replacement and/or repair with support vendor

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Initial deployment and configurations
- Device must be fully operational so that remote management capability can be configured

- Vendor hardware/software support contract or coverage required for support escalation and updates
- Ensure Company is an authorized caller associated with the vendor support contract
- Ensure Company is provided with vendor support contract contact information
- Client must provide the physical space, power, cabling, console connectivity, etc
- Client must provide remote personnel and access for activities requiring physical presence.

500098 Meraki Remote Office Management (1 Meraki Security/1 Meraki Switch/3 Meraki Aps): (requires Meraki Cloud Management)

Company's Responsibilities and Included Features

- Meraki Access Point Management (x3):
  - Configure, monitor, and troubleshoot access points
  - Manage replacement and/or repair with support vendor
- Meraki Primary Firewall Management (x1):
  - Firewall Management
  - Address translation (NAT/PAT) configuration
  - Firewall rule management (5 changes per month)
  - Cluster configuration (if needed)
  - VPN setting configurations (5 changes per month)
  - Supports local DB and LDAP authentication
  - Monitor and troubleshoot firewall
  - Update/patch firewall
  - Manage replacement and/or repair with support vendor
- Meraki Primary Switch Management (x1):
  - Meraki Layer 2 Switch Management
  - Spanning tree configuration
  - VLAN Assignment
  - Port Assignment
  - Etherchannel configuration and management
  - 802.1Q VLAN Trunk configuration and management
  - Monitor and troubleshoot switch
  - Update/patch switch
  - Manage replacement and/or repair with support vendor

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Meraki Access Point Management (x3):
  - Initial deployment and configurations
  - Device must be fully operational so that remote management capability can be configured
  - Vendor hardware/software support contract or coverage required for support escalation and updates
  - Ensure Company is an authorized caller associated with the vendor support contract
  - Ensure Company is provided with vendor support contract contact information
  - Client must provide the physical space, power, cabling, console connectivity, etc
  - Client must provide remote personnel and access for activities requiring physical presence
  - End-user wireless support
- Meraki Primary Firewall Management (x1):
  - Initial deployment and configurations

        - Device must be fully operational so that remote management capability can be configured
        - Vendor hardware/software support contract or coverage required for support escalation and updates
        - Ensure Company is an authorized caller associated with the vendor support contract
        - Ensure Company is provided with vendor support contract contact information
        - Client must provide the physical space, power, cabling, console connectivity, etc
        - Client must provide remote personnel and access for activities requiring physical presence
        - Internet/Intranet connectivity with sufficient bandwidth for operations and management requirements
    - Meraki Primary Switch Management (x1):
        - Initial deployment and configurations
        - Device must be fully operational so that remote management capability can be configured
        - Vendor hardware/software support contract or coverage required for support escalation and updates
        - Ensure Company is an authorized caller associated with the vendor support contract
        - Ensure Company is provided with vendor support contract contact information
        - Client must provide the physical space, power, cabling, console connectivity, etc
        - Client must provide remote personnel and access for activities requiring physical presence

500147 Circuit Management add on (Requires terminating device be covered under management)

Company's Responsibilities and Included Features

Circuit Management (Single circuit per device)

- Monitor circuit for up/down status
- Report on circuit bandwidth utilization via monitoring on managed router
- Error and discard reporting
- Identify outages and escalate to circuit vendor by opening trouble ticket
- Escalate trouble tickets with vendor following Company standard operating procedure
- Requires LOA with carrier to open tickets on client s behalf

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hardware Maintenance Coverage

- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that Company is an authorized caller to maintenance service providers Remote Hardware Support
- Provide remote hands-on support if physical intervention is required for troubleshooting

600047 Dedicated Layer-2/3 Switch Management (additional 48 ports)

Company's Responsibilities and Included Features

Additional Port Management

- Management of additional switch ports as per the base switch device management service item. Requires(MS-ND-SW3 or MS-ND-SW as the base)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

None

600049 Network Load Balancer Virtual Appliance Management

Company's Responsibilities and Included Features

Maintain Application Rules

Configure unique application flows (up to 20):

- Load balanced IP
- Real server configuration
- Pattern match rules
- Redirect rules

Software Management

Global device configuration including:

- Management IP (if needed)
- Basic device parameters
- AAA configuration
- NTP Service Configuration (if needed)

Troubleshooting of IOS\OS issues
IOS\OS patch\upgrade management
Configuration Backups

Virtual Appliance Maintenance Management

- Manage hardware replacement and or repair with hardware vendor
- Perform analysis of any hardware additions or upgrades

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hardware Maintenance Coverage

- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that Company is an authorized caller to maintenance service providers

600050 Wide Area Network Service Provider Management

Company's Responsibilities and Included Features

Circuit Management (Single circuit per device)

- Monitor circuit for up/down status
- Report on circuit bandwidth utilization via monitoring on managed router
- Error and discard reporting on managed router
- Identify outages and escalate to circuit vendor by opening trouble ticket
- Escalate trouble tickets with vendor following Company standard operating procedure
- Requires LOA with carrier to open tickets on client s behalf

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Circuit Termination Hardware Maintenance

- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that Company is an authorized caller to maintenance service providers Remote Hardware Support
- Provide remote hands-on support if physical intervention is required for troubleshooting
- Requires terminating device be covered under Company managed services

600107 Unmanaged Device Up/Down Monitoring

Company's Responsibilities and Included Features

Unmanaged Server Availability Monitoring

- Up-Down monitoring of server operating system
- Escalation to Client

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

601763 Dedicated Citrix ADC VPX Management (per pair)

Company's Responsibilities and Included Features

Administration

- Administration of a single or a clustered pair of Citrix ADC VPX appliances (Appliance)
- Citrix ADC configuration management for Virtual Apps and Desktops Gateway
- Administration of traffic and authentication policies
- Gateway virtual IP (VIP) management
- Administration of XML broker, load balancing, LDAP/LDAPS load balancing, storefront load balancing SSL, and director load balancing SSL
- Certificate management
- Periodic SSL hardening of profile for external facing VIPs
    - Periodic review of critical firmware and patches
    - Application of firmware updates and patches during Client provided and approved maintenance windows**
- Protocol optimization review and tuning
- Monitoring of Citrix ADC availability

** If Client does not provide Company with a maintenance window to apply upgrades and patches within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows

for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Appliance Incident Triage and Troubleshooting

- Triage of Appliance incidents
- Troubleshoot and work to resolve Appliance incidents
- Document Appliance issues and errors

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Citrix ADC Advanced configuration for:

- Load balanced VIPs not described above
- Authentication, Authorization, and Auditing of VIPs
- Content switching VIPs
- Web Application Firewall
- Unified gateway

Provide required public SSL certificate(s)

Procurement of necessary Citrix licensing, including any user access licensing

601938 Azure Application Gateway Administration

Company s Responsibilities and Included Features

Company will provide administration of an Azure Application Gateway within a Microsoft Azure subscription as described herein.

Administration

- Configuring and managing basic and path-based routing rules to manage traffic
- Adding or removing servers from backend pools as needed
- Configuring and managing backend settings
- Updating listeners as per changes in application endpoints
- Managing Secure Sockets Layer (SSL) certificates
- Configuring and managing health probes to monitor the health of the backend servers
- Scaling the Application Gateway on request by Client
- Document applicable Application Gateway resource, administration procedures and policies
- Backup of Application Gateway configuration to Azure storage repository

Security Administration

- Managing access permissions for the Application Gateway
- Azure Advisor Secure score review

Incident Triage and Troubleshooting

- Diagnosis of service incidents
- Triage of service incidents
- Troubleshoot and work to resolve service incidents
- Document service incidents
- Escalate incidents to Microsoft as needed

Monitoring

- Reviewing and acting on health probe results
- Monitoring Application Gateway performance and availability
- Setting up alerts for potential performance issues
- Availability and reliability monitoring
- Performance monitoring
- Events monitoring

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Microsoft Azure Subscription

- Azure subscription and resources
- Provide Azure monitoring resources for Azure Monitor and Log Analytics for service monitoring
- Provide Company access to subscriptions

Security and Audit

- SSL Certificate
- Provide audit requirements
- Provide Azure resources for audit logging

Application and Dependencies

- Managing and updating Web Application Firewall (WAF) policies
- Configuring SSL termination at the application gateway to offload the SSL decrypt/encrypt process
- Optimizing the Application Gateway for cost
- Application and content updates
- Third-party application dependencies

Deployment

- Creation and deployment of new Application Gateways and instances
- Repurpose or migration of Application Gateways

End User Support

- Support of non-Expert Users (typically refers to non-IT department staff or application end users)

Category: Managed Security

100288 Dedicated Security Appliance/Firewall Management (up to 500 rules)

Company's Responsibilities and Included Features

Basic Firewall Management Basic firewall rules including:

- Address translation (NAT/PAT)
- Firewall rule management
- Cluster configuration (if needed)
- L2L VPN tunnel configuration and support
- RAVPN (client based or anyconnect; only when firewall is NOT contextualized) configuration and support
- Supports local DB and LDAP authentication Hardware Maintenance Management
- Manage hardware replacement and/or repair with hardware vendor
- Perform analysis of any hardware additions or upgrades
- Apply hardware IOS\OS updates as necessary Remote Access VPN Management Deployment and support of client based remote access VPN including:
    - Group policy definitions
    - External user database authentication integration
    - Certificate management
    - Client VPN access utilizing CISCO Client software
    - Limited to 20 named users if local device authentication is used Site-to-site VPN Management
    - Management of the VPN Tunnel configurations on one side of a Point-to-Point VPN connection
    - Troubleshooting/support of VPN tunnel establishment

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hardware Maintenance Coverage

- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that Company is an authorized caller to maintenance service providers Internet Connectivity
- Internet connectivity with sufficient bandwidth

,Hardware Maintenance Coverage
- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that OneNeck is an authorized caller to maintenance service providers

Internet Connectivity
- Internet connectivity with sufficient bandwidth

500061 Meraki Primary Firewall Management

Company's Responsibilities and Included Features

- Configuration management (5 change requests per month limit)
- Address translation (NAT/PAT) configuration
- Firewall rule management (5 change requests per month limit)
- SD-WAN configuration management (5 change requests per month limit)
- Cluster configuration (if needed)
- VPN setting configurations (5 change requests per month limit)
- Monitor and troubleshoot firewall
- Update/patch firewall
- Manage replacement and/or repair with support vendor

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Initial deployment and configurations
- Device must be fully operational so that remote management capability can be configured
- Vendor hardware/software support contract or coverage required for support escalation and updates
- Ensure Company is an authorized caller associated with the vendor support contract
- Ensure Company is provided with vendor support contract contact information
- Client must provide the physical space, power, cabling, console connectivity, etc
- Client must provide remote personnel and access for activities requiring physical presence
- Internet/Intranet connectivity with sufficient bandwidth for operations and management requirements

500062 Meraki Secondary Firewall Management (requires Meraki Primary Firewall Management)

Company's Responsibilities and Included Features

Firewall Management

- Address translation (NAT/PAT) configuration
- Firewall rule management (5 changes per month)
- Cluster configuration (if needed)
- VPN setting configurations (5 changes per month)
- Monitor troubleshoot firewall
- Update/patch firewall
- Manage replacement and/or repair with support vendor

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Initial deployment and configurations
- Device must be fully operational so that remote management capability can be configured
- Vendor hardware/software support contract or coverage required for support escalation and updates
- Ensure Company is an authorized caller associated with the vendor support contract
- Ensure Company is provided with vendor support contract contact information
- Client must provide the physical space, power, cabling, console connectivity, etc
- Client must provide remote personnel and access for activities requiring physical presence
- Internet/Intranet connectivity with sufficient bandwidth for operations and management requirements.

500180 Cisco NextGen Firewall Management with IPS Support

Company's Responsibilities and Included Features

Firewall Management

- LAN to LAN VPN tunnel configuration and support, limited to a total of 5 VPN tunnel configurations per month
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of remote access VPN management vendor software including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing Cisco client software
    - Site-to-site VPN management
        - Deployment and administration of the VPN tunnel configurations on one side of a site-to-site VPN connection
        - Troubleshooting / support of VPN tunnel establishment
- Vendor-provided NGFW policy updates (application control)
- Schedule standard reports (make recipient modifications if necessary)
- Hardware Maintenance Management (if applicable)
    - Manage hardware replacement and/or repair with hardware vendor
    - Perform analysis of any hardware additions or upgrades
    - Apply hardware IOS\OS updates as necessary

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Firepower IPS (Intrusion Prevention System)

The following firewall support services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts and updates are functioning

Support Services on Company-Managed Operating Systems (OS)

- Troubleshoot security incidents specific to Company-Managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Identification of moves/adds/changes and deletions to be performed by Company.

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

Hardware Maintenance Coverage

- Procurement of hardware maintenance
- Provide contract numbers and phone numbers of applicable hardware maintenance service providers
- Ensure that Company is an authorized caller to maintenance service providers

End User License Agreement

Client agrees that the Cisco NGFWv Base + Threat software, and therefore Client s use of this Service as pertains to that software is subject to the Cisco End User License Agreement available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco Terms").

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at Company or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Cisco Intellectual Property rights including pursuing an action against any breaching third parties.

600364 Microsoft Windows Remote Access Services Management

Company's Responsibilities and Included Features

Windows Remote Access Services (RAS) administration

- Add, change, delete user RAS permissions
- RAS port management
- RAS service monitoring
- Requires Company management of the Windows server operating system on which RAS is running
- Requires Company management of the Client's Windows Active Directory

Incident Triage and Troubleshooting

- Triage of system incidents
- Troubleshooting of system incidents
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues
- Provide client with updates
- Document user issues and system errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating system software licensing

- Procurement of OS software and licensing for current version of operating system, including any user access licensing
- Providing software media for installation
- Procurement of current software maintenance where applicable

End user support

- Support of non-expert OS users (Typically refers to non-IT department staff or application end users)

601852 Managed Cisco Secure Endpoint Licenses and Support Service (formerly called Cisco AMP for Endpoints)

Cisco Secure Endpoint is a cloud-based advanced malware analysis and protection solution that allows users to conduct metadata file analysis to detect malware and cyber threats.

Notwithstanding the Term of this Statement of Work, this Service is provided for a minimum of 12 months. Company may revise terms of use or pricing at any time to reflect changes to terms or pricing by Cisco.

Definitions

Endpoint(s): any device capable of processing data and that can access a network, including but not limited to personal computers, mobile devices and network computer workstations.

Intellectual Property: any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Company's Responsibilities and Included Features

Licenses

Provide Cisco Secure Endpoint Licenses up to the quantity as stated in the Pricing Details above. Endpoint Licenses will be provided on a monthly subscription basis and must be implemented and deployed prior to use by Client.

- License Restrictions. This ItemID provides a license, not a transfer of title, to the Cisco Secure Endpoint Licenses. Cisco retains ownership of all copies of the Cisco Secure Endpoint License and related software and documentation. Client acknowledges that the Cisco Secure Endpoint software and documentation contain trade secrets of Cisco, its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Unless expressly authorized in writing by Cisco or otherwise permitted under applicable law, Client will not:
    - a. sell, resell, transfer, sublicense, or assign its license rights under this SOW;
    - b. modify, adapt or create derivative works;
    - c. reverse engineer, decompile, decrypt, disassemble or otherwise attempt to derive source code;
    - d. Use the Cisco Secure Endpoint software that is licensed for a specific device, whether physical or virtual, on another device;
    - e. remove, modify, or conceal any product identification, copyright, proprietary, intellectual property notices or other marks;
    - f. Use the Cisco Secure Endpoint software on secondhand or refurbished Cisco equipment not authorized by Cisco;
    - g. locate the Cisco Secure Endpoint software in Brazil, Russia, India and/or mainland China, unless mutually agreed in writing by the parties and authorized by Cisco;
    - h. Use any Cisco provided content or data other than with the Cisco Secure Endpoint software and any third-party products or services that Cisco has identified as compatible with the Cisco Secure Endpoint software;

Service Metering

- This is a metered service billed in arrears on a monthly basis.
- Endpoints connected to the Cisco Secure Endpoint Cloud for 16 days or more in the previous month are billable for the full month. Endpoints used for 15 days or fewer in a given month will not be charged for that month.
- Company may back bill Client for any error that results in an under-billing to Client within 180 days of the issuance of the invoice that should have reflected the under-billed usage. If Client has any reason to dispute an invoice, Client must notify Company in writing of any such disputed fees within 10 days of the invoice date and provide OneNeck with written details about why Client disputes the invoice.

Cisco Threat Response. Secure Endpoint includes access to Cisco Threat Response. Please see the Cisco Threat Response Privacy Data Sheet (https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=Privacy%20Data%20Sheet|Privacy%20Data%20Map) regarding any personal data processed by Cisco Threat Response. .

Cisco Secure Endpoint Support Services

- Conduct periodic reviews of Endpoint protection agents and associated policies
- Monitor security events and escalate incidents on non-Company-managed OSs to Client

The following Cisco Secure Endpoint Support Services will be performed upon Client request:

- Tune policies quarterly (adding exceptions, allowlisting, blocklisting)
- Monitor/maintain Endpoint protection agents through Secure Endpoint dashboard
- Manage file, directory and process exclusions policies
- Manage exception process for agent tampering protection
- Escalate issues as necessary to Cisco TAC (Technical Assistance Center)

Cisco Secure Endpoint Support Services on Company-Managed Operating Systems (OS)

The following services are included on Company-managed OSs only:

- Apply updates to existing Endpoint protection agents
- Alert-based detection response including:
    - 24 x 7 1st level triage
    - Escalation to Client response team per OneNeck Customer Operations Handbook
    - Post alert investigation and recommendations for Client action which may include the following actions by Company or Client:
        - Review logs for unusual accounts or connections
        - Verify users on systems are approved
        - Identify new admin accounts
        - Review event logs for anomalies
        - Verify log files are intact
        - Check for new entries in tasks scheduler
        - Identify recent software installed
        - Document most recent patch level and any exceptions
        - Document most recent AV update and signature

Reporting

- Provide and review selected Cisco Secure Endpoint reports with Client at least once per quarter
- Provide security incident digest reports monthly
- Review policies applied to Endpoint protection agents with Client on a periodic basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Intellectual Property in and to the Services belonging to Cisco or other Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party.

Warranties. NEITHER COMPANY NOR CISCO REPRESENT OR WARRANT THAT THE MANAGED CISCO AMP FOR ENDPOINTS LICENSES AND/OR SUPPORT SERVICE WILL GUARANTEE ABSOLUTE SECURITY DUE TO THE CONTINUAL DEVELOPMENT OF NEW

TECHNIQUES FOR INTRUDING UPON AND ATTACKING FILES, NETWORKS AND ENDPOINTS. NEITHER COMPANY NOR CISCO REPRESENT OR WARRANT THAT THE CLOUD SERVICES WILL PROTECT ALL OF CLIENT S FILES, NETWORK, OR ENDPOINTS FROM ALL MALWARE, VIRUSES OR THIRD- PARTY MALICIOUS ATTACKS. NEITHER COMPANY NOR CISCO MAKE ANY REPRESENTATIONS OR WARRANTIES REGARDING ANY THIRD-PARTY SYSTEM OR SERVICE TO WHICH THIS MANAGED CISCO AMP FOR ENDPOINTS AND SUPPORT SERVICE INTEGRATES OR TO ANY ONGOING INTEGRATION SUPPORT. INTEGRATIONS MADE ACCESSIBLE TO CLIENT THAT ARE NOT A GENERALLY AVAILABLE PRODUCT INCLUDED ON YOUR ORDER ARE PROVIDED ON AN "AS IS" BASIS.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless contracted separately with Company under this or another Executed Order, Client is responsible for the following:

- Implementation and deployment are not included in this ItemID, and must be contracted separately with Company. Client may not use Endpoint Licenses which have not been implemented and deployed.
- When assigning any names (policy, group, exclusion, etc.) with the exception of Computer name, Client may not use ON- at the beginning of the name. The ON- designation is reserved for Company usage only.
- Notify Company of any Cisco Secure Endpoint service issues
- Allow access to any devices to be connected to Secure Endpoint software
- Allow configuration of firewall rules required for access to the Cisco Secure Endpoint Cloud
- Designate a primary Client contact for security incident escalations
- Security Incident Event Management (SIEM) services

End User License Agreement

The Cisco Secure Endpoint service is subject to the applicable Cisco End User License Agreement located at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/cisco_end_user_license_agreement-eng.pdf ("Cisco EULA"). Client acknowledges and accepts that its subscription to and use of this Service is subject to the Cisco Terms.

Breach

Client shall notify Company promptly of any breach or suspected breach of the Cisco Terms or any third party license and further agrees that it will, at OneNeck or Cisco request, assist Cisco in efforts to preserve Cisco s or its supplier s Intellectual Property rights including pursuing an action against any breaching third parties.

601960 Managed Next Generation Palo Alto Firewall Service (PA-3220)

Company's Responsibilities and Included Features

Next Generation Firewall (NGFW) Management

- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of remote access VPN management vendor software including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing vendor software
    - Site-to-site VPN management
        - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection

Troubleshooting / support of VPN tunnel establishment

- Vendor-provided NGFW policy updates (application control)
- Schedule standard reports (make recipient modifications if necessary)

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat Prevention and WildFire

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat Prevention and WildFire
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot security incidents specific to Company-Managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Identification of moves/adds/changes and deletions to be performed by Company relating to Threat Prevention and WildFire.

SOC Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting

- Security gap analysis
- Threat intelligence collection and analysis

602357 Managed Next Generation Palo Alto Firewall Service (PA-5220)

Company's Responsibilities and Included Features

Next Generation Firewall (NGFW) Management

- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of remote access VPN management vendor software including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing vendor software
    - Site-to-site VPN management
        - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
        - Troubleshooting / support of VPN tunnel establishment
- Vendor-provided NGFW policy updates (application control)
- Schedule standard reports (make recipient modifications if necessary)

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat Prevention, GlobalProtect, DNS Security, URL Filtering and WildFire

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat Prevention, GlobalProtect, DNS Security, URL Filtering and WildFire
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot security incidents specific to Company-Managed applications and devices

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Identification of moves/adds/changes and deletions to be performed by Company relating to Threat Prevention, GlobalProtect, DNS Security, URL Filtering and WildFire..

SOC Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

602525 Managed Next Generation Palo Alto Firewall Services for HA Pair

Company managed services for a high-availability (HA) pair of Palo Alto firewall appliances with Palo Alto software subscriptions for Threat Prevention, GlobalProtect, DNS Security, PANDB URL Filtering and WildFire; configured as active/standby .

Company's Responsibilities and Included Features

Next Generation Firewall (NGFW) Management

- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of remote access VPN management vendor software including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management

Client VPN access utilizing vendor software
    - Site-to-site VPN management
        - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
        - Troubleshooting / support of VPN tunnel establishment
- Vendor-provided NGFW policy updates (application control)
- Schedule standard reports (make recipient modifications if necessary)

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat Prevention, GlobalProtect, DNS Security, URL Filtering and WildFire

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat Prevention, GlobalProtect, DNS Security, URL Filtering and WildFire
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts and updates are functioning

NGFW Events for Company-Managed Operating Systems (OS)

- Troubleshoot security incidents specific to Company-Managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

All product licensing supported by the aforementioned services Company will provide.

Identification of moves/adds/changes and deletions to be performed by Company relating to Threat Prevention, GlobalProtect, DNS Security, URL Filtering and WildFire.

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

602739 Managed Next Generation Palo Alto Security Appliance Pair (PA-3250)

Company managed services for a high-availability (HA) pair of Palo Alto firewall appliances configured as active/standby and Palo Alto software subscriptions for Threat Prevention, URL Filtering and WildFire.

Company's Responsibilities and Included Features

Next Generation Firewall (NGFW) Management

- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of remote access VPN management vendor software including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing vendor software
    - Site-to-site VPN management
        - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
        - Troubleshooting / support of VPN tunnel establishment
- Vendor-provided NGFW policy updates (application control)
- Schedule standard reports (make recipient modifications if necessary)

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat Prevention, URL Filtering and WildFire

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat Prevention, URL Filtering and WildFire
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot security incidents specific to Company-Managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

All product licensing supported by the aforementioned services Company will provide.

Identification of moves/adds/changes and deletions to be performed by Company relating to Threat Prevention, URL Filtering and WildFire.

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

602741 Nutanix Flow Security Policies Management 10 Pack

Definitions

Address Group: A grouping of IP address, or ranges used in the definition of security policies

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Categories: A logical grouping of VMs. Security policies are applied to the Categories.

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Nutanix Flow Security: A policy-driven security framework that inspects traffic within the data center. The framework uses a workload-centric approach instead of a network-centric approach. Therefore, it can scrutinize traffic to and from VMs no matter how their network configurations change and where they reside in the data center.

Nutanix Flow Service: A group of network protocol-port combinations. Services are leveraged in the policy creation workflow

Company's Responsibilities and Included Features

Nutanix Flow Security Policies Management 10 Pack provides managed service support for up to (10) ten Nutanix Flow security policies and application of Nutanix Flow Security software updates, patches and upgrades. Company provides support for the following Network Flow Security policy types:

- Application security policy
- Isolation environment policy
- Quarantine policy
- VDI policy

Service Exclusions:

Creation of new security policies is not included under this scope of Services. New security policy creation services available from Company under different ItemId numbers.

Nutanix Flow Security Administration:

- Configuration of whitelist-based policy expressions
- Apply or modify enforcement modes
- Category values management for the purpose of supporting security policies
- Nutanix Flow Service management
    - Application, creation or modification of Nutanix Flow Services
    - Troubleshooting traffic flows between policies
- Creation and modification of address groups.
- Application of filtering and grouping to security policy
- Manage ad hoc exports snapshots of the working security configuration and imports
- Upon Client request, configure syslog monitoring for policy hit logs to a Client provided syslog server.

Flow Security Software Patching, Updates, and Upgrades:

- Periodic reviews of patches, updates and upgrades (Updates)
- Manage change order process including Client notification of Updates
- Application of Updates during Company defined maintenance windows
- Periodic application of the Updates to the Nutanix Flow Security software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices.

Metered Service:

- This service is metered
- The unit of measure is up to ten (10) security policies per 10-Pack
- All security policies within the cluster must be managed
- The quantity of 10-Packs is calculated on the maximum number of security polices identified within the Cluster per month, divided by 10, and rounded up to the largest whole number.

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Platform Requirements:

- Cluster must be running AHV on AOS 5.6 or later
- All Nodes in the Cluster must be licensed for Nutanix Flow
- Prism central instance must be hosted on one of the AHV clusters registered with it.
- The Kafka container used to store data that is required for flow visualization to work and must not be deleted.
- VDI policies require the use of a domain controller, Client must provide the domain controller and service credentials to authenticate into the account.

Policy Creation:

- Contract with Company under separate ItemID and defined scope of work for new security policy creation.
- Specify which VMs belong to the application to be protected
- Identify the entities or networks in the inbound and outbound directions that communication needs to be allowed for
- Review and verify deployment requirements, constraints, assumptions, dependencies and decisions for configuration.

Policy Validation:

- Validate that policy protected applications function as expected

Security Operations Center (SOC) Services:

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix Flow Security is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.

- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

603157 Next Generation Palo Alto Firewall Administration - Basic

Company's Responsibilities and Included Features

Next Generation Firewall (NGFW) Management

- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support

- Support Client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of remote access VPN management vendor software including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing vendor software
    - Site-to-site VPN management
        - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection
        - Troubleshooting / support of VPN tunnel establishment
- Vendor-provided NGFW policy updates (application control)
- Schedule standard reports (make recipient modifications if necessary)

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

SOC Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services

- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

Additional Functionality Configuration and Management

Provide management of the following, if installed or used:

- Threat prevention
- Malware protection
- URL filtering

Licensing and Hardware Maintenance Coverage

- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Ensure that Company is an authorized caller to maintenance service providers

- License and provide Company access to Panorama - Centralized Firewall Management

Client Premises Environmentals and Remote Hands

- Where the firewall is not in a Company data center
    - Client will provide adequate power, environmental, physical security, and network connections.
    - Provide designated on-site data center hands and eyes under the direction of a Company administrator on Company request to execute tasks such as:
        - Rack and connect the device
        - Turning the firewall off or on
        - Provide accompanied access to the device for maintenance technicians

603492 Managed Next Generation Palo Alto Security Appliance

Company managed services for a Palo Alto firewall appliance that has Palo Alto software subscriptions for Threat Prevention, URL Filtering and WildFire.

Company's Responsibilities and Included Features

Next Generation Firewall (NGFW) Management

- LAN to LAN VPN tunnel configuration and support
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of remote access VPN management vendor software including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing vendor software
    - Site-to-site VPN management
        - Management of the VPN tunnel configurations on one side of a site-to-site VPN connection

Troubleshooting / support of VPN tunnel establishment

- Vendor-provided NGFW policy updates (application control)
- Schedule standard reports (make recipient modifications if necessary)

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Support Services for Threat Prevention, URL Filtering and WildFire

The following NGFW Support Services will be performed upon Client request:

- Support and troubleshoot perimeter intrusion prevention and detection (ingress/egress)
- Client-identified moves/adds/changes and deletions relating to Threat Prevention, URL Filtering and WildFire
- Configuration and delivery of standard reports (non-custom)
- Confirm that reports, alerts and updates are functioning

NGFW Services on Company-Managed Operating Systems (OS)

- Troubleshoot security incidents specific to Company-Managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

All product licensing supported by the aforementioned services.

Identification of moves/adds/changes and deletions to be performed by Company relating to Threat Prevention, URL Filtering and WildFire.

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Security incident response

- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting
- Security gap analysis
- Threat intelligence collection and analysis

603495 Cisco Duo User Provisioning Administration (MACD)

Cisco Duo User Provisioning Administration (MACD) provides move, add, change, delete services for managing the assignment of Cisco Duo to users on behalf of Client.

606984 Cisco NextGen Firewall Management without IPS Support

Company's Responsibilities and Included Features

Firewall Management

- LAN to LAN VPN tunnel configuration and support, limited to a total of 5 VPN tunnel configurations per month
- Remote access VPN configuration and support
- Support Client-provided authentication integration including:
    - Local Database
    - Lightweight Directory Access Portal (LDAP)
    - Authentication, Authorization and Accounting (AAA)
    - Active Directory (AD)
    - Multifactor authentication (MFA)
    - Security Information and event Management (SIEM)
- Remote access VPN management
    - Deployment and support of remote access VPN management vendor software including:
        - Group policy definitions
        - External user database authentication integration
        - Certificate management
        - Client VPN access utilizing Cisco client software
    - Site-to-site VPN management
        - Deployment and administration of the VPN tunnel configurations on one side of a site-to-site VPN connection
        - Troubleshooting / support of VPN tunnel establishment
- Vendor-provided NGFW policy updates (application control)
- Schedule standard reports (make recipient modifications if necessary)
- Hardware Maintenance Management (if applicable)
    - Manage hardware replacement and/or repair with hardware vendor
    - Perform analysis of any hardware additions or upgrades
    - Apply hardware IOS\OS updates as necessary

Patching and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Application of updates and patches during Client approved maintenance windows
- Periodic next version analysis and recommendations (upon Client request)
- Periodic upgrades to the NGFW software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices

If Client does not provide Company with a maintenance window to apply upgrades and patches (critical and security) within a commercially reasonable timeframe based on the severity of the upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to upgrade or patch, and any applicable service level agreements will be suspended until such time as patching and upgrades are up to date. If patching or upgrading is delayed by more than

three (3) months, a catch-up patching process will be applied at the time patching resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades or patches, thus limiting the Company from applying upgrades and patches.

Virtualization Platform

Provide a virtualization platform to host the virtual firewall management system

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide Internet access for the firewall management system

Support Services on Company-Managed Operating Systems (OS)

- Troubleshoot security incidents specific to Company-Managed applications and devices

Expert User technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

General Terms

Cisco Intellectual Property. The Intellectual Property of Client and Company shall be as provided in the Master Services Agreement. Notwithstanding any other provision of this SOW or the Master Services Agreement, as between Client, Company and Cisco, Cisco shall at all times retain all right, title, and interest in and to all pre-existing Cisco Intellectual Property owned by Cisco as of the Effective Date of this SOW and all Cisco Intellectual Property in and to the Services belonging to Cisco or other Cisco Intellectual Property provided or developed by Cisco or a third party on Cisco s behalf thereafter. Third party hardware and software shall at all times be owned by the applicable third party. Cisco Intellectual Property shall mean any and all tangible and intangible (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

,

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Identification of moves/adds/changes and deletions to be performed by Company.

Security Operations Center (SOC) Services

Perform security operations services including but not limited to:

- Security incident response
- SIEM or centralized logging configuration services
- Security incident identification, containment, analysis, investigation and reporting
- Data breach investigation and reporting

- Security gap analysis
- Threat intelligence collection and analysis

Hardware Maintenance Coverage

- Procurement of hardware maintenance
- Provide contract numbers and phone numbers of applicable hardware maintenance service providers
- Ensure that Company is an authorized caller to maintenance service providers

,150.0,150.0,300.0,0.0%,300.0,300.0,50.0%, 462

Category: Managed Servers

100051 VMware Host Server Management

Company's Responsibilities and Included Features

Administration

- Troubleshoot VMware software issues
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks
- Virtual machine provisioning/de-provisioning
- Management of vSwitch network
- Management of vStorage network
- Management of ESX host servers through vCenter
- Administration of all built-in VMware dependency components
- Managing high availability groups
- Performing VM vMotions and Storage vMotions where required
- Utilization reporting

Support and Access

- Delegated access to vCenter management platform to manage VM s if needed.
- Provide monitoring visibility into the performance of the host machines.
- Provide notification to Client of any critical host level issues, if required

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of any service requirements, changes or modifications.
- Application licensing and supporting maintenance including the hypvervisor, virtual machine operating system licensing and support maintenance.
- Deployment and configuration of operating systems in VMs
- Ownership and management of application and operating system support and management of VMs.
- Backup services
- Management of underlying hardware

103050-N Managed Linux Server Setup

Company's Responsibilities and Included Features

- Prepare and configure virtual container (networking, disk, tools)
- OS installation, configuration and OS updates/patches
- 3rd party tool installation (backup, monitoring)

- Documentation updates (portal, tasks, support center)
- Configure and verify backups and monitoring
- Create and configure VM container (if applicable)
- Firmware updates (if applicable)
- OS install

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

103051-N Managed Windows 2003/2008 Server Setup

Company's Responsibilities and Included Features

- Prepare and configure virtual container (networking, disk, tools)
- OS installation, configuration and OS updates/ patches
- 3rd party tool installation (backup, anti-virus, monitoring)
- Documentation updates (portal, tasks, support center)
- Create and configure VM container (if applicable)
- Firmware updates (if applicable)
- Configure and verify backups and monitoring

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

103055-N Windows Server Decommission

Company's Responsibilities and Included Features

- Final backup
- Uninstall monitoring, backup software, request related policies to be deactivated
- Remove server from domain
- Update hardware list, task list, documentation
- Worked with shared services and network to reclaim IP address, remove from DNS, remove all monitoring and backups, reclaim storage (if applicable)
- Remove server from information databases

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

600057 Oracle VM Host Server administration

Company's Responsibilities and Included Features

System Administration

System administration of Oracle VM (hypervisor) including:

- Hypervisor configuration
- Hypervisor monitoring
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks
- Virtual machine provisioning
- Management of Oracle VM server through Oracle VM Manager
- Management of Oracle VM Manager application

Hypervisor System Upgrade, Update and Patch Management

- Periodic review and application of Oracle VM hypervisor patches or updates.
- Application of patches and minor release updates.
- A minor release is a release of a product that does not add significant new features or content and is primarily a bundle of performance or bug fix patches.
- Major release (x and .x) upgrades will be provided on a time and material basis contracted under a separate statement of work (SOW).
- Client must provide the Company an opportunity to patch or deploy patches and minor updates to the environment within 90 days of Company notifying the Client of the need to patch or update the environment otherwise any SLA s on the environment or systems reliant on this service will be waived.
- Required compute and storage hardware upgrades may necessitate major or minor release updates to the hypervisor.

Server Incident Triage and Troubleshooting

- Triage of server hardware or hypervisor system incidents
- Troubleshooting of server hardware or hypervisor system incidents
- Document incidents and hypervisor system errors

Hardware Maintenance Management

- Manage hardware replacement and or repair with hardware vendor
- Perform analysis of any hardware additions or upgrades
- Apply hardware BIOS updates as necessary

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hypervisor System Software Licensing

- Procurement of software and licensing for current version of hypervisor (Oracle VM), including any user access licensing where applicable
- Providing software media for installation
- Procurement of current software maintenance where applicable

Guest Operating Systems

- Procurement of software and licensing for current version of guest operating systems, including any user access licensing where applicable
- Procurement of current operating system maintenance where available
- Management of guest operating systems

Hardware Maintenance Coverage

- Procurement of hardware maintenance for the duration of the SOW
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that Company is an authorized caller to maintenance service providers

Third Party Oracle VM Utilities and Applications

- Management of third party Oracle VM enhancement tools, utilities or applications

End User Support

- Support of non-expert OS users (Typically refers to non-IT department staff or application end users)

600149 Linux Physical Server DR replication administration - Client SW based replication solution

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the operating system administration of a server in a Recovery Site acting as a failover server and the replication of the necessary data from the primary server to the target DR server for disaster recovery purposes.
Replication of the server file systems from the primary server to the target DR server is to be provided through the use of server to server replication software.
Company shall develop and maintain Disaster Recovery Failover Procedures for the server.

Replication Software Patch Management

- Replication Software patch management of both the primary and target DR servers
- Up to quarterly routine review same-version patch analysis and application
- Application of updates and patches during approved maintenance windows
- Up to one application version upgrade every two years

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Server Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of planned failover tests per year is limited to the "Number of DR tests per year" referenced in Pricing Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the

data was when testing began.

Server Failover Services

- On declaration of a disaster, Company will perform the steps necessary to activate the target DR server and make it the active server, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the active server, administration of the server will be as per the administrative, support, backup and monitoring services as defined for the primary server

Server Failback Services

- When the ability to provide services from the primary server is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the primary site.
- Reestablishment of replication back to the target DR server will then be activated and services will return back to normal operational mode
- Server Failback Services will be provided on a project, time and material basis

DR Linux Server Monitoring

Configuration of monitoring thresholds and parameters

- Monitoring and reporting of key metrics including:
- Disk space usage
- Disk IO
- Hardware logs
- Special plug-ins (like PowerPath)
- Processor load
- Memory usage
- Processes (abandoned and run-away)
- Server availability

DR Server Incident Triage and Troubleshooting

- Triage of server hardware or operating system incidents
- Troubleshooting of server hardware or operating system incidents

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Hardware Maintenance Management

- Manage hardware replacement and or repair with hardware vendor
- Perform analysis of any hardware additions or upgrades

Apply hardware BIOS updates as necessary

DR Operating System Upgrades

- Upgrades to new major version of the operating system or embedded OS application will be provided on a project time and material basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Virus Protection Software Licensing

- Procurement of virus protection software and licensing for current version of virus protection system
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Hardware Maintenance Coverage

- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that Company is an authorized caller to maintenance service providers

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

DR Backup Infrastructure (Tape or Disk based)

During normal operation, no backups will be performed on the target DR server; however during a failover, normal backups should be done and thus one of the following backup solutions must be provided:

- Backup system to enable backup of data from this server to tape or disk, including:
- Backup server and agent licensing
- Available disk storage and tape media if required

OR

- Contracted usage of the Company Centralized Backup service

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

Remote Server Network Access

- If the DR Target server is not housed in a Company data center, the Client must provide secure remote network access to the server to enable management of the server, independent of the primary data center network, in the case a disaster is called.

Operating System Software Licensing

Procurement of OS software and licensing for current version of operating system, including any user access licensing

- Providing software media for installation
- Procurement of current software maintenance where applicable

600150 MS Windows Physical Server DR replication administration - Client SW based replication solution

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the operating system administration of a server in a Recovery Site acting as a failover server and the replication of the necessary data from the primary server to the target DR server for disaster recovery purposes.
Replication of the server file systems from the primary server to the target DR server is to be provided through the use of server to server replication software.
Company shall develop and maintain Disaster Recovery Failover Procedures for the server.

Replication Software Patch Management

- Replication Software patch management of both the primary and target DR servers
- Up to quarterly routine review same-version patch analysis and application
- Application of updates and patches during approved maintenance windows
- Up to one application version upgrade every two years

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Server Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of planned failover tests per year is limited to the "Number of DR tests per year" referenced in Pricing Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the data was when testing began.

Server Failover Services

- On declaration of a disaster, Company will perform the steps necessary to activate the target DR server and make it the active server, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the active server, administration of the server will be as per the administrative, support, backup and monitoring services as defined for the primary server

Server Failback Services

- When the ability to provide services from the primary server is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the primary site.
- Reestablishment of replication back to the target DR server will then be activated and services will return back to normal operational mode
- Server Failback Services will be provided on a project, time and material basis

DR Windows Server Monitoring

Monitoring and reporting of key metrics including:

- Disk utilization
- Processor load
- Memory usage
- Automatically launched services
- Server Availability

DR Server Incident Triage and Troubleshooting

- Triage of server hardware or operating system incidents
- Troubleshooting of server hardware or operating system incidents

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Hardware Maintenance Management

- Manage hardware replacement and or repair with hardware vendor
- Perform analysis of any hardware additions or upgrades
- Apply hardware BIOS updates as necessary

DR Operating System Upgrades

- Upgrades to new major version of the operating system or embedded OS application will be provided on a project time and material basis

Virus Protection Software

Procurement of Company standard virus protection software for operating system where required.
Providing software media for installation, maintenance and configuration of the software

Antivirus management of file systems and operating system

- Installation of a managed Antivirus console
- Application of updates and patches to the antivirus software on server platforms only
- Configuration and validation of virus protection and scanning on server platforms only

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Virus Protection Software Licensing

- Procurement of virus protection software and licensing for current version of virus protection system
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Hardware Maintenance Coverage

- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Insure that Company is an authorized caller to maintenance service providers

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

DR Backup Infrastructure (Tape or Disk based)

During normal operation, no backups will be performed on the target DR server; however during a failover, normal backups should be done and thus one of the following backup solutions must be provided:

- Backup system to enable backup of data from this server to tape or disk, including:
- Backup server and agent licensing
- Available disk storage and tape media if required

OR

- Contracted usage of the Company Centralized Backup service

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

Remote Server Network Access

- If the DR Target server is not housed in a Company data center, the Client must provide secure remote network access to the server to enable management of the server, independent of the primary data center network, in the case a disaster is called.

Operating System Software Licensing*

Procurement of OS software and licensing for current version of operating system, including any user access licensing
Providing software media for installation
Procurement of current software maintenance where applicable
* Workstations/Servers deployed on Company's VPS platform include a license for any supported version of Microsoft Server

600151 Linux Server virtual machine disaster recovery administration - Client SW Based replication solution

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the operating system administration of a server in a Recovery Site acting as a failover server and the replication of the necessary data from the primary server to the target DR server for disaster recovery purposes.
Replication of the server file systems from the primary server to the target DR server is to be provided through the use of server to server replication software.
Company shall develop and maintain Disaster Recovery Failover Procedures for the server.

Replication Software Patch Management

- Replication Software patch management of both the primary and target DR servers
- Up to quarterly routine review same-version patch analysis and application
- Application of updates and patches during approved maintenance windows
- Up to one application version upgrade every two years

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Server Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of planned failover tests per year is limited to the "Number of DR tests per year" referenced in Pricing Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the data was when testing began.

Server Failover Services

- On declaration of a disaster, Company will perform the steps necessary to activate the target DR server and make it the active server, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the active server, administration of the server will be as per the administrative, support, backup and monitoring services as defined for the primary server

Server Failback Services

- When the ability to provide services from the primary server is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the primary site.
- Reestablishment of replication back to the target DR server will then be activated and services will return back to normal operational mode
- Server Failback Services will be provided on a project, time and material basis

DR Linux Server Monitoring

Configuration of monitoring thresholds and parameters

- Monitoring and reporting of key metrics including:
- Disk space usage
- Disk IO
- Hardware logs
- Special plug-ins (like PowerPath)
- Processor load
- Memory usage
- Processes (abandoned and run-away)
- Server availability

DR Server Incident Triage and Troubleshooting

- Triage of server hardware or operating system incidents
- Troubleshooting of server hardware or operating system incidents

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

DR Operating System Upgrades

- Upgrades to new major version of the operating system or embedded OS application will be provided on a project time and material basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Virtualization Platform

- Server host hardware (Disk, CPU and RAM)
- Virtualization software on which the virtual machine being managed is run
- Management of virtualization platform

Virus Protection Software Licensing

- Procurement of virus protection software and licensing for current version of virus protection system
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

DR Backup Infrastructure (Tape or Disk based)

During normal operation, no backups will be performed on the target DR server; however during a failover, normal backups should be done and thus one of the following backup solutions must be provided:

- Backup system to enable backup of data from this server to tape or disk, including:
- Backup server and agent licensing
- Available disk storage and tape media if required

OR

- Contracted usage of the Company Centralized Backup service

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

Remote Server Network Access

- If the DR Target server is not housed in a Company data center, the Client must provide secure remote network access to the server to enable management of the server, independent of the primary data center network, in the case a disaster is called.

Operating System Software Licensing

- Procurement of OS software and licensing for current version of operating system, including any user access licensing
- Providing software media for installation
- Procurement of current software maintenance where applicable

600152 Linux Server virtual machine disaster recovery administration - SAN Based replication solution

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the operating system administration of a server in a Recovery Site acting as a failover server and the replication of the necessary data from the primary server to the target DR server for disaster recovery purposes.
Replication of the server file systems from the primary server to the target DR server is to be provided through the use of SAN based replication.
Company shall develop and maintain Disaster Recovery Failover Procedures for the server.

SAN Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Server Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of planned failover tests per year is limited to the "Number of DR tests per year" referenced in Pricing Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the data was when testing began.

Server Failover Services

- On declaration of a disaster, Company will perform the steps necessary to activate the target DR server and make it the active server, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the active server, administration of the server will be as per the administrative, support, backup and monitoring services as defined for the primary server

Server Failback Services

- When the ability to provide services from the primary server is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the primary site.
- Reestablishment of replication back to the target DR server will then be activated and services will return back to normal operational mode
- Server Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Virtualization Platform

- Server host hardware (Disk, CPU and RAM)
- Virtualization software on which the virtual machine being managed is run
- Management of virtualization platform

SAN Replication Infrastructure, Software and Licensing

- Provisioning of SAN replication infrastructure (source and destination).
- Provisioning of SAN replication software and licensing for current version of replication software/infrastructure
- Procurement of current hardware and software maintenance where applicable

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

DR Backup Infrastructure (Tape or Disk based)

During normal operation, no backups will be performed on the target DR server; however during a failover, normal backups should be done and thus one of the following backup solutions must be provided:

- Backup system to enable backup of data from this server to tape or disk, including:
- Backup server and agent licensing
- Available disk storage and tape media if required

OR

- Contracted usage of the Company Centralized Backup service

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

Remote Server Network Access

- If the DR Target server is not housed in a Company data center, the Client must provide secure remote network access to the server to enable management of the server, independent of the primary data center network, in the case a disaster is called.

600154 MS Windows Server virtual machine disaster recovery administration - Backup Based replication solution

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the operating system administration of a server in a Recovery Site acting as a failover server for disaster recovery purposes.

Recovery of the server file systems from the primary server to the target DR server is to be provided through the use of backup tape recovery from the primary servers.

During normal operation the DR server will remain in a shutdown state, except for periodic patching and testing of the DR plan.

Company shall develop and maintain Disaster Recovery Failover Procedures for the server.

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Server Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of planned failover tests per year is limited to the "Number of DR tests per year" referenced in Pricing Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the data was when testing began.

Server Failover Services

- On declaration of a disaster, Company will perform the steps necessary to activate the target DR server and make it the active server, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the active server, administration of the server will be as per the administrative, support, backup and monitoring services as defined for the primary server

Server Failback Services

- When the ability to provide services from the primary server is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the primary site.
- Reestablishment of replication back to the target DR server will then be activated and services will return back to normal operational mode
- Server Failback Services will be provided on a project, time and material basis

DR Windows Server Monitoring

Monitoring and reporting of key metrics including:

- Disk utilization
- Processor load
- Memory usage

- Automatically launched services
- Server Availability

DR Server Incident Triage and Troubleshooting

- Triage of server hardware or operating system incidents
- Troubleshooting of server hardware or operating system incidents

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

DR Operating System Upgrades

- Upgrades to new major version of the operating system or embedded OS application will be provided on a project time and material basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Virtualization Platform

- Server host hardware (Disk, CPU and RAM)
- Virtualization software on which the virtual machine being managed is run
- Management of virtualization platform

DR Backup Infrastructure (Tape or Disk based)

During normal operation, no backups will be performed on the target DR server; however during a failover, normal backups should be done and thus one of the following backup solutions must be provided:

- Backup system to enable backup of data from this server to tape or disk, including:
- Backup server and agent licensing
- Available disk storage and tape media if required

OR

- Contracted usage of the Company Centralized Backup service

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

Remote Server Network Access

- If the DR Target server is not housed in a Company data center, the Client must provide secure remote network access

to the server to enable management of the server, independent of the primary data center network, in the case a disaster is called.

Operating System Software Licensing*

Procurement of OS software and licensing for current version of operating system, including any user access licensing
Providing software media for installation
Procurement of current software maintenance where applicable
* Workstations/Servers deployed on Company's VPS platform include a license for any supported version of Microsoft Server

600155 MS Windows Server virtual machine disaster recovery administration - Client SW Based replication solution

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the operating system administration of a server in a Recovery Site acting as a failover server and the replication of the necessary data from the primary server to the target DR server for disaster recovery purposes.
Replication of the server file systems from the primary server to the target DR server is to be provided through the use of server to server replication software.
Company shall develop and maintain Disaster Recovery Failover Procedures for the server.

Replication Software Patch Management

- Replication Software patch management of both the primary and target DR servers
- Up to quarterly routine review same-version patch analysis and application
- Application of updates and patches during approved maintenance windows
- Up to one application version upgrade every two years

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Server Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of planned failover tests per year is limited to the "Number of DR tests per year" referenced in Pricing

Parameters

- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the data was when testing began.

Server Failover Services

- On declaration of a disaster, Company will perform the steps necessary to activate the target DR server and make it the active server, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the active server, administration of the server will be as per the administrative, support, backup and monitoring services as defined for the primary server

Server Failback Services

- When the ability to provide services from the primary server is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the primary site.
- Reestablishment of replication back to the target DR server will then be activated and services will return back to normal operational mode
- Server Failback Services will be provided on a project, time and material basis

DR Windows Server Monitoring

Monitoring and reporting of key metrics including:

- Disk utilization
- Processor load
- Memory usage
- Automatically launched services
- Server Availability

DR Server Incident Triage and Troubleshooting

- Triage of server hardware or operating system incidents
- Troubleshooting of server hardware or operating system incidents

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Virus Protection Software

Procurement of Company standard virus protection software for operating system where required.
Providing software media for installation, maintenance and configuration of the software

DR Operating System Upgrades

- Upgrades to new major version of the operating system or embedded OS application will be provided on a project time and material basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Virtualization Platform

- Server host hardware (Disk, CPU and RAM)
- Virtualization software on which the virtual machine being managed is run
- Management of virtualization platform

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

DR Backup Infrastructure (Tape or Disk based)

During normal operation, no backups will be performed on the target DR server; however during a failover, normal backups should be done and thus one of the following backup solutions must be provided:

- Backup system to enable backup of data from this server to tape or disk, including:
- Backup server and agent licensing
- Available disk storage and tape media if required

OR

- Contracted usage of the Company Centralized Backup service

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

Remote Server Network Access

- If the DR Target server is not housed in a Company data center, the Client must provide secure remote network access to the server to enable management of the server, independent of the primary data center network, in the case a disaster is called.

Operating System Software Licensing*

Procurement of OS software and licensing for current version of operating system, including any user access licensing
Providing software media for installation
Procurement of current software maintenance where applicable
* Workstations/Servers deployed on Company's VPS platform include a license for any supported version of Microsoft Server

600156 MS Windows Server virtual machine disaster recovery administration - SAN Based replication solution

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the operating system administration of a server in a Recovery Site acting as a failover server and the replication of the necessary data from the primary server to the target DR server for disaster recovery purposes.

Replication of the server file systems from the primary server to the target DR server is to be provided through the use of SAN based replication.

Company shall develop and maintain Disaster Recovery Failover Procedures for the server.

SAN Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service is referenced in Pricing Parameters
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is referenced in Pricing Parameters

Server Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of planned failover tests per year is limited to the "Number of DR tests per year" referenced in Pricing Parameters
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the data was when testing began.

Server Failover Services

- On declaration of a disaster, Company will perform the steps necessary to activate the target DR server and make it the active server, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the active server, administration of the server will be as per the administrative, support, backup and monitoring services as defined for the primary server

Server Failback Services

- When the ability to provide services from the primary server is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the primary site.
- Reestablishment of replication back to the target DR server will then be activated and services will return back to normal operational mode
- Server Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Virtualization Platform

- Server host hardware (Disk, CPU and RAM)
- Virtualization software on which the virtual machine being managed is run
- Management of virtualization platform

SAN Replication Infrastructure, Software and Licensing

- Provisioning of SAN replication infrastructure (source and destination).
- Provisioning of SAN replication software and licensing for current version of replication software/infrastructure
- Procurement of current hardware and software maintenance where applicable

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

DR Backup Infrastructure (Tape or Disk based)

During normal operation, no backups will be performed on the target DR server; however during a failover, normal backups should be done and thus one of the following backup solutions must be provided:

- Backup system to enable backup of data from this server to tape or disk, including:
- Backup server and agent licensing
- Available disk storage and tape media if required

OR

- Contracted usage of the Company Centralized Backup service

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

Remote Server Network Access

- If the DR Target server is not housed in a Company data center, the Client must provide secure remote network access to the server to enable management of the server, independent of the primary data center network, in the case a disaster is called.

Company's Responsibilities and Included Features

General

Company shall provide Disaster Recovery Services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the operating system administration of a server in a Recovery Site acting as a failover server and the replication of the necessary data from the primary server to the target DR server for disaster recovery purposes.

Replication of the server file systems from the primary server to the target DR server is to be provided through the use of server to server replication software.

Company shall develop and maintain Disaster Recovery Failover Procedures for the server.

Replication Software Patch Management

- Replication Software patch management of both the primary and target DR servers
- Up to quarterly routine review same-version patch analysis and application
- Application of updates and patches during approved maintenance windows
- Up to one application version upgrade every two years

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The RPO for this service can be defined after deployment when the impact of available network bandwidth and network latency has been established.
- The replication policies for this service will be configured to achieve this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is 4 hours.

Server Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of planned failover tests per year is limited to one (1) tests per year.
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster ocurr during a test the data will be as old as the data was when testing began.

Server Failover Services

- On declaration of a disaster, Company will perform the steps necessary to activate the target DR server and make it the active server, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the active server, administration of the server will be as per the

administrative, support, backup and monitoring services as defined for the primary server

Server Failback Services

- When the ability to provide services from the primary server is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the primary site.
- Reestablishment of replication back to the target DR server will then be activated and services will return back to normal operational mode
- Server Failback Services will be provided on a project, time and material basis

DR Server Incident Triage and Troubleshooting

- Triage of server hardware or operating system incidents
- Troubleshooting of server hardware or operating system incidents

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Virtualization Platform

- Server host hardware (Disk, CPU and RAM)
- Virtualization software on which the virtual machine being managed is run
- Management of virtualization platform

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

DR Backup Infrastructure (Tape or Disk based)

During normal operation, no backups will be performed on the target DR server; however during a failover, normal backups should be done and thus one of the following backup solutions must be provided:

- Backup system to enable backup of data from this server to tape or disk, including:
- Backup server and agent licensing
- Available disk storage and tape media if required

OR

- Contracted usage of the Company Centralized Backup service

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

Remote Server Network Access

- If the DR Target server is not housed in a Company data center, the Client must provide secure remote network access to the server to enable management of the server, independent of the primary data center network, in the case a disaster is called.

Operating System Software Licensing*

Procurement of OS software and licensing for current version of operating system, including any user access licensing
Providing software media for installation
Procurement of current software maintenance where applicable
* Workstations/Servers deployed on Company's VPS platform include a license for any supported version of Microsoft Server

600158 MS Windows Server virtual machine disaster recovery administration - Hypervisor based replication solution

Company's Responsibilities and Included Features

General

Company shall provide disaster recovery services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center. This service is specific to the operating system administration of a server in a recovery site acting as a failover server and the replication of the necessary data from the primary server to the target DR server for disaster recovery purposes.
Replication of the server file systems from the primary server to the target DR server is to be provided through the use of hypervisor based replication software.
Company shall develop and maintain disaster recovery failover procedures for the server.

Replication Software Patch Management

- Replication Software patch management of both the primary and target DR servers
- Up to quarterly routine review same-version patch analysis and application
- Application of updates and patches during approved maintenance windows
- Up to one application version upgrade every two years

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.

The RPO for this service can be defined after deployment when the impact of available network bandwidth and network latency has been established.

- The replication policies for this service will be configured to manage to this this RPO; however this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service is 4 hours.

Server Failover Testing

- Periodic failover testing for this service will be conducted in collaboration with the Client.
- The number of planned failover tests per year is limited to one (1) tests per year.
- During failover testing the Disaster Recovery systems will not be receiving updated replication data from the production system thus the RPO will not be met and should a disaster occurr during a test the data will be as old as the data was when testing began.

Server Fail-over Services

- On declaration of a disaster, Company will perform the steps necessary to activate the target DR server and make it the active server, operational and accessible on the DR network as defined in the disaster eecovery failover procedures.
- During the period that the target DR server is acting as the active server, administration of the server will be as per the administrative, support, backup and monitoring services as defined for the primary server

Server Fail-back Services

- When the ability to provide services from the primary server is restored, Company will initiate fail-back to the primary server as documented in the disaster recovery failover procedures, and in collaboration with the Client, schedule and return service back to the primary site.
- Reestablishment of replication back to the target DR server will then be activated and services will return back to normal operational mode
- Server fail-back services will be provided on a project, time and material basis

DR Server Incident Triage and Troubleshooting

- Triage of server hardware or operating system incidents
- Troubleshooting of server hardware or operating system incidents

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Virtualization Platform

- Server host hardware (Disk, CPU and RAM)
- Virtualization software on which the virtual machine being managed is run
- Management of virtualization platform

Replication Software Licensing

- Procurement of replication software and licensing for current version of replication software
- Providing software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

DR Backup Infrastructure (Tape or Disk based)

During normal operation, no backups will be performed on the target DR server; however during a failover, normal backups should be done and thus one of the following backup solutions must be provided:

- Backup system to enable backup of data from this server to tape or disk, including:
- Backup server and agent licensing
- Available disk storage and tape media if required

OR

- Contracted usage of the Company Centralized Backup service

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

Remote Server Network Access

- If the DR Target server is not housed in a Company data center, the Client must provide secure remote network access to the server to enable management of the server, independent of the primary data center network, in the case a disaster is called.

Operating System Software Licensing

Procurement of OS software and licensing for current version of operating system, including any user access licensing where applicable.
Procurement of current software maintenance where applicable.

600188 Unmanaged Server Detail Monitoring

Company's Responsibilities and Included Features

Unmanaged Detail Device Monitoring

- Up-Down monitoring of device
- Agent based performance monitoring integrated into the Company monitoring system
- SNMP monitoring.
- Access to performance monitoring data through the Company Client Portal
- Escalation to Client based upon specific alert thresholds

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Device Management

- Full responsibility for managing device

600241 Microsoft Windows Virtual Server Setup

Company's Responsibilities and Included Features

- Prepare and configure virtual container (Networking, compute, disk, tools).
- Install and configure operating system.
- Apply patches to bring server up to date.
- Install and configure backup, anti-virus, monitoring.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide configuration requirements based on purpose of server.

600346 Azure Site Recovery Replication Management

Company's Responsibilities and Included Features

Overview

Client has selected Azure Site Recovery (ASR) to provide Disaster Recovery (DR) services to provide service continuity in the event of a failure that prevents the delivery of services from the primary data center. Client requires Company to monitor and manage these services on behalf of Client.

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of Microsoft support

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backwards from the point of disaster.
- The replication policies for this service will be configured to achieve an agreed upon RPO; however, this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating

system is operational and available on the DR network
- The RTO for this service will be defined after the first DR test

Server Failover Testing

- DR failover testing for this server will be conducted in collaboration with the Client.
- Server failover testing will be provided on a project, time and material basis
- DR failover testing must be scheduled at least 1 calendar month in advance.

Server Failover Services

- On declaration of a disaster, Company will perform the steps necessary to activate the target DR server and make it the active server, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR server is acting as the active server, administration of the server will be as per the administrative, support, backup and monitoring services as defined for the primary server

Server Failback Services

- When the ability to provide services from the primary server is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the primary site.
- Reestablishment of replication back to the target DR server will then be activated and services will return to normal operational mode
- Server Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Expert-to-expert helpdesk support:

- 24 x 7 technical support for priority 1 and 2 incidents
- 8 x 5 technical support for priority 3,4 and 5 incidents

* An Expert User is defined as an application or system knowledge holder and a single point of contact for escalating incidents to Company limited to 5 total defined experts or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Azure Resources

An Azure subscription with the following services:

- Azure Site Recovery
- Storage Services
- ExpressRoute or VPN services

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

Client Side DR Configuration and Testing

- Configurations of end user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.

600622 Physical Server Hardware Management

Company's Responsibilities and Included Features

Server Hardware Management

Server hardware management is only provided on:

- Physical servers
- Company approved server hardware platforms
- Servers with Client procured hardware maintenance support from hardware vendor or third-party hardware maintenance support provider

Server hardware management includes:

- Triage, diagnosis and work to resolve hardware issues
- Management of hardware replacement and/or repair with applicable hardware vendor
- Analysis of any hardware additions or upgrades
- Application of hardware firmware updates as necessary

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Operating system or hypervisor management
- Procurement of hardware maintenance for the duration of the MSA
- Provide a designated on-site resource where the server is not in a Company data center, to do the following where applicable:
  - Rack and connect device
  - Backup tape handling
  - Provide accompanied access to the device for maintenance technicians
  - Provide ad hoc on-site non-technical hand and eyes support under direction of a Company administrator to assist in physical device management

601391 Azure Site Recovery Replication Management

Company's Responsibilities and Included Features

Overview

Client has selected Azure Site Recovery (ASR) to provide Disaster Recovery (DR) services to provide

service continuity in the event of a failure that prevents the delivery of services from the primary data center. Client requires Company to monitor and manage these services on behalf of Client.

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of Microsoft support

Recovery Point Objective (RPO) Management

- The definition of RPO is the maximum amount of data that will be unavailable in the DR system in terms of time, backward from the point of disaster.
- The replication policies for this service will be configured to achieve an agreed upon RPO; however, this will be limited by the network bandwidth available for replication of data from the primary server to the target DR server.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network
- The RTO for this service will be defined after the first DR test

Server Failover Testing

- DR failover testing for this server will be conducted in collaboration with the Client.
- Server failover testing will be provided on a project, time and material basis
- DR failover testing must be scheduled at least 1 calendar month in advance.
- Company is limited to bringing up the servers only and performing either a ping test or ARM console validation under boot diagnostics.

Server Failover Services

- On declaration of a disaster, Company will perform the steps necessary to activate the target DR server and make it the active server, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- Company is limited to bringing up the servers only and performing either a ping test or ARM console validation under boot diagnostics.
- During the period that the target DR server is acting as the active server, administration of the server will be as per the administrative, support, backup and monitoring services as defined for the primary server

Server Failback Services

- When the ability to provide services from the primary server is restored, Company will initiate failback to the primary server as documented in the Disaster Recovery Failover Procedures, and in collaboration with the Client, schedule and return service back to the primary site.
- Reestablishment of replication back to the target DR server will then be activated and services

will return to normal operational mode
- Server Failback Services will be provided on a project, time and material basis

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Business Continuity / Disaster Recovery Plan

- A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

Azure Resources

- An Azure subscription with the following services:
  - Azure Site Recovery
  - Storage Services
  - ExpressRoute or VPN services

Replication Network

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

Client Side DR Configuration and Testing

- Configurations of end-user devices and/or Client infrastructure required to allow end users to access the environment.
- Responsible for conducting functional and data validation test during server failover testing.
- Client-side network changes

DR Workload Configuration and Testing

- Configuration, testing and management of the operating system, databases, and applications during:
  - Failover testing
  - DR failover
  - DR failback

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking, and virtualization services

Block: A chassis that contains a single or multiple Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

Nutanix AOS Base Features Management is quantified as per Node.

AOS Administration

Company will support administration of the following base features of AOS:

- Enterprise storage
  - Cluster sizing including heterogeneous Clusters
  - Data tiering
  - Inline compression
  - Inline performance deduplication
  - Online Cluster growth
  - Compression *
  - Deduplication *
  - Erasure coding (EC-X) **
- Infrastructure Resilience
  - Data path redundancy
  - Tunable redundancy factor
- Security
  - Client authentication
  - Cluster lockdown
  - Data-at-rest encryption (software-based and self-encrypting drives)
- Management and analytics
  - Prism Central and Prism Elements
  - Pulse
  - Cluster health

*Features that require a higher level of Nutanix AOS licensing such as AOS Pro, AOS Ultimate, or Prism Pro

** Erasure coding is a feature available to Clusters comprised of at least 5 Nodes. Its use may not be appropriate in all configurations and is dependent upon the workloads. Company will consult with Client to determine the appropriate Cluster level settings to meet their business, workload performance, and availability goals.

Administration of additional AOS features is not included under this scope of Services but may be available from Company under different ItemId numbers

Cluster and Node Incident Triage and Troubleshooting

- Triage of Node or Block hardware or operating system incidents
- Troubleshooting and work to resolve Node hardware or operating system incidents
- Document user issues and AOS errors

Patching, Updates and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the AOS software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable timeframe based on the severity of the updates, patches or upgrades, Client waives any and all claims against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updates and upgrades are up to date. If patching, updating or upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time updating, patching or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for upgrades, updates or patches.

Block and Node Maintenance Management

Block and Node maintenance management is limited to:

- Physical Blocks and Nodes
- Company and Nutanix-approved server hardware platforms
- Hardware with Client-procured hardware maintenance support subscription
- Periodic reviews of critical patches

Block and Node Maintenance Management

- Management of hardware replacement and/or repair with hardware vendor
- Analysis of hardware additions or upgrades
- Application of hardware BIOS updates as necessary

Exoert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Own and manage guest virtual machine (VM) applications and operating systems support
- Perform all data backup
- Manage network devices
- Remediate Company identified platform deployment issues prior to Company taking ownership of the platform administration
- Migrate physical machines and VMs on or off platforms
- Client is responsible for all disaster recovery solutions and associated services
- Client is responsible for all third-party utilities and applications including but not limited to management of third-party enhancement tools, utilities or applications

Hardware and Software Licensing and Maintenance Coverage

- Procure all application licensing including but not limited to Nutanix AOS, hypervisor, and virtual machine operating systems
- Procure and maintain hardware and software maintenance for the duration of the SOW
- Provide contract numbers and phone numbers for applicable hardware and software maintenance service providers
- Ensure that Company is an authorized caller to maintenance service providers

Client Premises Remote Hands

- Where the Node is not in a Company data center, provide a designated on-site resource to do the following on Company request
  - Rack and connect device
  - Handle backup tapes
  - Provide accompanied access to the device for maintenance technicians
  - Provide ad hoc on-site non-technical hand and eyes support under the direction of a Company administrator to assist in physical device management

601496

Definitions

AHV: Nutanix Acropolis Hypervisor

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

Block: A chassis that contains one or more Nodes

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Company's Responsibilities and Included Features

AHV Administration

Company will support administration of the following base features of AHV:

- Enterprise storage
  - Virtual Machine (VM) centric snapshots and clones
  - VM-centric Storage QoS *
  - VM Flash Mode *
- Data Protection
  - Application consistent snapshots
  - Local snapshots
  - Self-service restores
  - Asynchronous replication with a minimum 1-hour recovery point objective (RPO)
- Virtualization Features
  - VM management. VM s operating system management and application management is specifically excluded from this scope.
  - VM automated resource scheduling
  - VM affinity rules
  - Virtual network configuration
  - Host profiles
  - VM high availability

Self-service portal

*Features that require a higher level of Nutanix AOS licensing such as AOS Ultimate, AOS Pro, or Prism Pro

Administration of additional AHV features is not included under this scope of services but may be available from Company under different ItemId numbers

AHV Triage and Troubleshooting

- Triage of AHV system incidents
- Troubleshoot and work to resolve AHV system incidents
- Document AHV system issues and errors

Hypervisor (AHV) Patching, Updates and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the AHV software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable timeframe based on the severity of the update, upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updating and upgrades are up to date. If patching, updating or upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time patching, updating or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for updates, upgrades and/or patches.

Co-administration

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
    - Cluster and VM performance and analysis
    - Cluster and health and availability
    - Cluster capacity and trend info
    - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
    - Create, delete and modify VMs
    - Execute snapshots and restorations
    - Add VMs to catalog
    - Import, add, create and delete images to catalog
    - Create and modify data protection and recovery policies

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the

OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Client required to contract with Company for Nutanix AOS Base Features Management
- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Remediate Company identified platform deployment issues prior to Company taking ownership of the platform administration
- Migrate physical machines and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment (Management VMs)
- Open necessary network and firewall ports to provide Company access to Management VMs
- Provide VPN termination point for Company to access Client s environment

Third Party Utilities and Applications

- Manage third-party AHV enhancement tools, utilities and applications

Hardware and Software Licensing and Maintenance Coverage

- Procure all application licensing including but not limited to the hypervisor and VM operating systems
- Procure and maintain hardware and software maintenance for the duration of the SOW
- Provide contract numbers and phone numbers for applicable hardware and software maintenance service providers
- Ensure that Company is an authorized caller to maintenance service providers

Client Premises Remote Hands

- Where the Node is not in a Company data center, provide a designated on-site resource to do the following on Company request
    - Rack and connect device
    - Handle backup tapes
    - Provide accompanied access to the device for maintenance technicians
    - Provide ad hoc on-site non-technical hand and eyes support under the direction of a Company administrator to assist in physical device management

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of the Nutanix AHV is by Nutanix, Inc. and may be subject to changes in provisioning and performance as determined by Nutanix, Inc.

- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.

601497

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services.

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services.

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged cluster. Nodes are generally purpose architected to meet IT infrastructure, application service and performance profiles.

VMware ESXi: VMware's hypervisor platform

Company's Responsibilities and Included Features

VMware System Administration

VMware ESXi Management on Nutanix AOS is quantified as per Node that participates within the Cluster. Company will perform the following Services on the applicable VMware systems:

- Configure operating system
- Perform preventative maintenance
- Perform emergency maintenance
- Provide performance tuning
- Perform server health checks
- Perform file system maintenance
- Provision Virtual machines
- Manage basic vSwitch network
- Manage advanced network switching (i.e. Cisco Nexus 1000V*)
- Manage basic vStorage network
- Manage VMware server through vCenter
- Manage vCenter application
- Administer built-in VMware dependency components
- Provide utilization reporting

LAN management of the virtual switch is specifically excluded.

VMware ESXi Triage and Troubleshooting

- Triage of VMware ESXi incidents
- Troubleshoot and work to resolve VMware ESXi system incidents
- Document VMware ESXi system issues and errors

VMware ESXi Patching, Updates and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the VMware ESXi software (including major upgrades) will be conducted at Company s discretion and in accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable timeframe based on the severity of the update, upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updates and upgrades are up to date. If patching, updating or upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time patching, updating or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for updates, upgrades or patches.

Co-administration

Company is providing managed services on a virtualization platform with an end-user experience making certain self-service

features available to Client including:

- Ability to login into vCenter and general visibility into the Cluster metrics and configuration settings such as as:
  - Cluster and VM performance and analysis
  - Cluster and health and availability
  - Cluster capacity and trend info
  - Alerts and notifications
- Creation of customized dashboards
- Self-service management of virtual infrastructure
  - Create, delete and modify VMs
  - Execute snapshots and restorations
  - Add VMs to catalog
  - Import, add, create and delete images to catalog
  - Create and modify data protection and recovery policies.

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes

- Client required to contract with Company for Nutanix AOS Base Features Management
- Own and manage guest VM applications and operating systems support
- Perform all data backup
- Manage network devices
- Remediate Company identified platform deployment issues prior to Company taking ownership of the platform administration
- Migrate physical and/or VMs onto or off of the platform
- Provide VM resources within the Cluster for Company s operating systems and applications that are used to managed the Client s environment (Management VMs)
- Open necessary network and firewall ports to provide Company access to Management VMs
- Provide VPN termination point for Company to access Client s environment

Third Party Utilities and Applications

- Manage third-party VMware enhancement tools, utilities and applications

Hardware and Software Maintenance Coverage

- Procure all application licensing including but not limited to the hypervisor and VM operating systems
- Procure and maintain hardware and software maintenance for the duration of the SOW
- Provide contract numbers and phone numbers for applicable hardware and software maintenance service providers
- Ensure that Company is an authorized caller to maintenance service providers

Client Premises Remote Hands

- Where the server is not in a Company data center, provide a designated on-site resource to do the following where applicable:
    - Rack and connect device
    - Handle backup tapes
    - Provide accompanied access to the device for maintenance technicians
    - Provide ad hoc on-site non-technical hand and eyes support under the direction of a Company administrator to assist in physical device management

Acknowledgment and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of the AOS is by Nutanix, Inc. and its provision and performance may be subject to change as determined by Nutanix, Inc.
- Client agrees, acknowledges, and understands that the actual manufacture of the VMware ESXi is by VMware, Inc. and its provision and performance may be subject to change as determined by VMware, Inc.
- Client agrees that Nutanix offerings provided herein are subject to the Nutanix License and Service Agreement available https://www.nutanix.com/legal/eula, which is hereby incorporated into this SOW in full.
- Client agrees that VMware ESXi offerings provided herein are subject to the VMware Services End User License Agreement available at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf and privacy policy located at https://www.vmware.com/help/privacy.html, which are hereby incorporated into this Statement of Work.

601907 Microsoft Windows Server Administration - VM

Company's Responsibilities and Included Features

General

Company will provide systems administration of a Microsoft Windows Server virtual machine (VM) as described herein.

System Administration

System administration of the server operating system (OS) including:

- OS configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks
- Start and stop services
- Document applicable OS administration procedures and policies

Built in OS Applications Administration

Administration of the following built-in OS components that are bundled with the OS:

- Performance monitor
- Device manager
- Windows Update service
- Windows Firewall

The following components are specifically excluded from administration under this ItemID:

- Remote Desktop Services (RDS)
- Licensing/Terminal Server Gateway

- SharePoint Services
- Active Directory Services/Application Directory Admin Mode/Active Directory Federation Services
- Server virtualization services
- Application server(s) -IIS/WWW-IIS/FTP-IIS/SMTP
- Certificate Services
- Certification Authority
- DHCP
- DNS
- WINS
- Distributed File System (DFS)
- File system management / DFS replication services
- Windows Deployment Services
- Failover Clustering
- Print Management

Windows Server Monitoring

- Install Company licensed monitoring agents where applicable
- Configure monitoring thresholds and parameters
- Monitor and report key metrics including:
-
    - Disk utilization
    - Processor load
    - Memory usage
    - Core OS services including such as:
        - Cryptographic Service
        - Local Session Manager
        - Remote Procedure Call (RPC)
        - Security Accounts Manager
        - Server
        - Task Scheduler
        - Windows Event Log
        - Windows Firewall
        - Windows Time
        - Workstation
    - Client may request application-level services monitoring with notification only. Development of application custom monitoring scripts may incur additional one-time fees, contracted on a separate time and materials project basis
    - Server availability

Windows Server Patch Administration- Level 1 Patch Baseline - Microsoft Critical and Security Update

- Monthly review of Microsoft Windows Server security updates
- Company will follow a change control process to include notice submission, approval and application of security updates, as further provided herein

This Level 1 Patch Baseline provides for application of Microsoft security updates for the following components:

- Cumulative security updates for core OS (applies to the latest Windows Server version only)
- Security only updates for core OS (applies to Windows Server versions other than the latest Windows Server version)
- Security only updates for .NET framework
- Therapeutic reboots

Client to provide at a minimum, a four (4) hours monthly patch window for patching plus an additional minimum of one and one-half (1.5) hours for each group of servers rebooted as a group

Client is limited to three (3) patch windows per month across all Windows Servers, unless mutually agreed upon by all Parties

If Client does not provide Company with an opportunity to apply the necessary critical and security updates, and patching is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes and Client may incur additional charges. Client acknowledges and accepts all risk of limiting the Company from applying security updates beyond the above three-month period.

For servers that are normally offline, Company will bring the server online monthly in order to apply OS patches during scheduled patching windows. These servers and their applications must allow for/support this monthly patching window, including bootup and shutdown of the server by both manual and automatic processes. Company understands the desire for certain servers to remain offline; however, Company is not responsible for resource usage costs incurred while the servers are online.

Server Incident Triage and Troubleshooting

- Triage of server OS incidents
- Troubleshoot and work to resolve server OS incidents
- Document system issues and OS errors

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage standard local OS security features

Operating System Upgrades

- Periodic next version analysis and recommendations
- Notifications of upcoming OS End of Life
- Upgrades to a new major version of the OS or embedded OS application are outside of the scope of this ItemID and may be provided on a separate time and materials project basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating System Software Licensing

- Procure OS software and licensing for current version of OS, including any user access licensing
- Procure current software maintenance where applicable

Note: Servers deployed on Company's public cloud, VPC or FLEX platforms include a license for any supported version of Microsoft Server

Virus Protection Software Licensing and Management

- Procure virus protection software and licensing and maintenance for current version of OS of the VM
- Manage antivirus software and updates
- Installation of antivirus software

Virtualization Platform

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide console access to the OS

Client Access Licensing

- End-user access licensing of OS or applications, if applicable

End User Support

- Support of non-expert OS users (typically refers to non-IT department staff or application end users)

Backup Job Administration and Backup Infrastructure (if server is required to be backed up)

Backup Job Administration

- Administration of server backup jobs
- Installing and maintaining agents
- Backup restores

Backup system to enable backup of data from this server:

- Contracted usage of the Company backup service which includes server backup job management

or

- Backup server and agent licensing with available disk storage and tape media, if required
- Administration of backup system
- Tape storage (if applicable)

601930 Microsoft Windows Server Administration - Physical Server

Company's Responsibilities and Included Features

General

Company will provide systems administration of a Microsoft Windows Server on a physical server as described herein.

System Administration

System administration of the server operating system (OS) including:

- OS configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks
- Start and stop services
- Document applicable OS administration procedures and policies

Built in OS Applications Management

Administration of the following built-in OS components that are bundled with the OS:

- Performance monitor
- Device manager
- Windows Update service

- Windows Firewall

The following components are specifically excluded from administration under this ItemID:

- Remote Desktop Services (RDS)
- Licensing/Terminal Server Gateway
- SharePoint Services
- Active Directory Services/Application Directory Admin Mode/Active Directory Federation Services
- Server virtualization services
- Application server(s) -IIS/WWW-IIS/FTP-IIS/SMTP
- Certificate Services
- Certification Authority
- DHCP
- DNS
- WINS
- Distributed File System (DFS)
- File system management / DFS replication services
- Windows Deployment Services
- Failover Clustering
- Print Management

Windows Server Monitoring

- Install Company licensed monitoring agents where applicable
- Configure monitoring thresholds and parameters
- Monitor and report key metrics including:
-
    - Disk utilization
    - Processor load
    - Memory usage
    - Core OS services including such as:
        - Cryptographic Service
        - Local Session Manager
        - Remote Procedure Call (RPC)
        - Security Accounts Manager
        - Server
        - Task Scheduler
        - Windows Event Log
        - Windows Firewall
        - Windows Time
        - Workstation
    - Client specific application services may be monitored on Client request and upon agreement by Company
    - Server availability

Windows Server Patch Management - Level 1 Patch Baseline - Microsoft Security Update

- Monthly review of Microsoft Windows Server critical and security updates
- Company will follow a change control process to include notice submission, approval and application of security updates, as further provided herein

This Level 1 Patch Baseline provides for application of Microsoft security updates for the following components:

- Cumulative security updates for core OS (applies to the latest Windows Server version only)
- Security only updates for core OS (applies to Windows Server versions other than the latest Windows Server version)
- Security only updates for .NET framework
- Therapeutic reboots

Client to provide at a minimum, a four (4) hours monthly patch window for patching plus an additional minimum of one and one-half (1.5) hours for each group of servers rebooted as a group

Client is limited to three (3) patch windows per month across all Windows Servers, unless mutually agreed upon by all Parties

If Client does not provide Company with an opportunity to apply the necessary critical and security updates, and patching is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes and Client may incur additional charges. Client acknowledges and accepts all risk of limiting the Company from applying security updates beyond the above three-month period.

For servers that are normally offline, Company will bring the server online monthly in order to apply OS patches during scheduled patching windows. These servers and their applications must allow for/support this monthly patching window, including bootup and shutdown of the server by both manual and automatic processes. Company understands the desire for certain servers to remain offline; however, Company is not responsible for resource usage costs incurred while the servers are online.

Hardware Maintenance Management

- Manage hardware part replacement and or repair with hardware vendor
- Apply hardware firmware updates as necessary
- Hardware upgrades or adding additional hardware components are outside of the scope of this ItemID and may be provided on a separate time and materials project basis

Server Incident Triage and Troubleshooting

- Triage of server OS and hardware incidents
- Troubleshoot and work to resolve server OS and hardware incidents
- Document system issues and OS and hardware errors

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Security Management Services

- Provide and maintain OS local user security and permissions
- Manage standard local OS security features

Operating System Upgrades

- Periodic next version analysis and recommendations
- Notifications of upcoming OS End of Life
- Upgrades to a new major version of the OS or embedded OS application are outside of the scope of this ItemID and may be provided on a separate time and materials project basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Out-of-Band Management Access

- Provide Company the ability to access the server over an out-of-band console/lights-out management console with the

ability to force a reboot and remotely power on the server

Operating System Software Licensing

- Procure OS software and licensing for current version of OS, including any user access licensing
- Procure current software maintenance where applicable

Hardware Maintenance Coverage

- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Ensure that Company is an authorized caller to maintenance service providers

Hardware Monitoring

- Monitoring of hardware components are outside of the scope of this ItemID

Client Premises Environmentals and Remote Hands

- Where the server is not in a Company data center
    - Client will provide adequate power, environmental, physical security, and network connections.
    - Provide designated on-site data center hands and eyes under the direction of a Company administrator on Company request to execute tasks such as:
        - Rack and connect device
        - Turning server off or on
        - Handle backup tapes
        - Provide accompanied access to the device for maintenance technicians

Virus Protection Software Licensing and Management

- Procure virus protection software and licensing and maintenance for current version of OS of the VM
- Manage antivirus software and updates
- Installation of antivirus software

Virtualization Platform

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software Manage virtualization platform
- Provide console access to the OS

Client Access Licensing

- End-user access licensing of OS or applications, if applicable

End User Support

- Support of non-expert OS users (typically refers to non-IT department staff or application end users)

Backup Job Management and Backup Infrastructure (if server is required to be backed up)

Backup Job Management

- Management of server backup jobs
- Installing and maintaining agents
- Backup restores

Backup system to enable backup of data from this server:

- Contracted usage of the Company backup service which includes server backup job management

or

- Backup server and agent licensing with available disk storage and tape media, if required
- Management of backup system
- Tape storage (if applicable)

601935 RHEL Linux Server Administration - VM

Company's Responsibilities and Included Features

General

Company will provide administration of a Red Hat Enterprise Linux (RHEL) virtual machine (VM) as described herein.

System Administration

System administration of the server operating system (OS) including:

- OS configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks
- Start and stop services/daemons/processes
- Document applicable OS administration procedures and policies

Built in OS Applications Administration

Administration of the following built-in OS components that may be bundled with the OS:

- SSH
- Firewall configuration
- NIC configuration

Excludes:

- Application server(s) - Examples: Apache/Tomcat(Java)/mySQL/postgresql/FTP
- Certificate services
- Certification authority
- Non-OS file systems replication services
- 3rd party application management
- SElinux
- Server used as Routed Firewall
- Print management
- SAMBA/CIF/Network file management
- SMTP management
- DNS management/BIND
- OS clustering
- GUI/Xserver
- DHCP
- Cron Job creation/modification
- Custom Script/Modules

Linux Server Monitoring

- Install monitoring agents where applicable
- Configure monitoring thresholds and parameters
- Monitor and report key metrics including:
    - Cron

        - Syslog
        - SSH
        - NTP
        - Server availability
    -
        - Disk utilization
        - Processor load
        - Memory usage
        - Server availability
        - Core OS services including such as:
- Client may request application-level services monitoring with notification only. Development of application custom monitoring scripts may incur additional one-time fees, contracted on a separate time and materials project basis

Linux Server Patch Administration of OS Security Updates

- Monthly review of OS vendor security updates
- Company will follow a change control process to include notice submission, approval and application of security updates, as further provided herein

Client to provide at a minimum, a four (4) hours monthly patch window for patching plus an additional minimum of one and one-half (1.5) hours for each group of servers rebooted as a group

Client is limited to three (3) patch windows per month across all servers, unless mutually agreed upon by all Parties

If Client does not provide Company with an opportunity to apply the necessary security updates, and patching is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes and Client may incur additional charges. Client acknowledges and accepts all risk of limiting the Company from applying security updates beyond the above three-month period.

For servers that are normally offline, Company will bring the server online monthly in order to apply OS patches during scheduled patching windows. These servers and their applications must allow for/support this monthly patching window, including bootup and shutdown of the server by both manual and automatic processes. Company understands the desire for certain servers to remain offline; however, Company is not responsible for resource usage costs incurred while the servers are online.

Server Incident Triage and Troubleshooting

- Triage of server OS incidents
- Troubleshoot and work to resolve server operating system incidents
- Document system issues and OS errors

Expert User Technical Support*

Expert-to-expert helpdesk support:

- 24 x 7 technical support for priority 1 and 2 incidents
- 8 am to 5 pm technical support for priority 3, 4 and 5 incidents

* An Expert User is defined as someone with in-depth application or system knowledge and a single point of contact for escalating incidents to Company. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage any standard OS security features

Operating System Upgrades

- Periodic next version analysis and recommendations

- Minor version upgrades available by request (Version.x upgrades)
- Major version upgrades that require a full rebuild of the system will be provided on time and materials project basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating System and Application Software Licensing

- Procure software and licensing for current version of OS, including any user access licensing
- Procure current OS software maintenance where applicable
- End-user access licensing
- Application and database licensing, if applicable

Virtualization Platform

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide console access to the OS

Virus Protection Software Licensing and Administration (if Client requires Virus Protection)

- Procure virus protection software and licensing and maintenance for current version of OS of the VM
- Manage antivirus software and updates
- Installation of antivirus software

End User Support

- Support of non-expert OS users (Typically refers to non-IT department staff or application end users)

Backup Job Administration and Backup Infrastructure (if server is required to be backed up)

Backup Job Administration

- Administration of server backup jobs
- Installing and maintaining agents
- Backup restores

Backup system to enable backup of data from this server:

- Contracted usage of the Company backup service which includes server backup job management

or

- Backup server and agent licensing with available disk storage and tape media, if required
- Administration of backup system
- Tape storage (if applicable)

601936 RHEL Linux Server Administration Physical Server

Company's Responsibilities and Included Features

General

Company will provide administration of a Red Hat Enterprise Linux (RHEL) server on a physical server as described herein.

System Administration

System administration of the server operating system (OS) including:

- OS configuration

- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks
- Start and stop services/daemons/processes
- Document applicable OS administration procedures and policies

Built in OS Applications Administration

Administration of the following built-in OS components that may be bundled with the OS:

- SSH
- Firewall configuration
- NIC configuration

Excludes:

- Application server(s) - Examples: Apache/Tomcat(Java)/mySQL/postgresql/FTP
- Certificate services
- Certification authority
- Non-OS file systems replication services
- 3rd party application management
- SElinux
- Server used as Routed Firewall
- Print management
- SAMBA/CIF/Network file management
- SMTP management
- DNS management/BIND
- OS clustering
- GUI/Xserver
- DHCP
- Cron Job creation/modification
- Custom Script/Modules

Linux Server Monitoring

- Install monitoring agents where applicable
- Configure monitoring thresholds and parameters
- Monitor and report key metrics including:
    - Cron
    - Syslog
    - SSH
    - NTP
    - Server availability
-
    - Disk utilization
    - Processor load
    - Memory usage
    - Server availability
    - Core OS services including such as:
- Client may request application-level services monitoring with notification only. Development of application custom monitoring scripts may incur additional one-time fees, contracted on a separate time and materials project basis

Linux Server Patch Administration of OS Security Updates

- Monthly review of OS vendor security updates
- Company will follow a change control process to include notice submission, approval and application of security

updates, as further provided herein

Client to provide at a minimum, a four (4) hours monthly patch window for patching plus an additional minimum of one and one-half (1.5) hours for each group of servers rebooted as a group

Client is limited to three (3) patch windows per month across all servers, unless mutually agreed upon by all Parties

If Client does not provide Company with an opportunity to apply the necessary security updates, and patching is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes and Client may incur additional charges. Client acknowledges and accepts all risk of limiting the Company from applying security updates beyond the above three-month period.

For servers that are normally offline, Company will bring the server online monthly in order to apply OS patches during scheduled patching windows. These servers and their applications must allow for/support this monthly patching window, including bootup and shutdown of the server by both manual and automatic processes. Company understands the desire for certain servers to remain offline; however, Company is not responsible for resource usage costs incurred while the servers are online.

Hardware Maintenance Management

- Manage hardware part replacement and or repair with hardware vendor
- Apply hardware firmware updates as necessary
- Hardware upgrades or adding additional hardware components are outside of the scope of this ItemID and may be provided on a separate time and materials project basis

Server Incident Triage and Troubleshooting

- Triage of server OS incidents
- Troubleshoot and work to resolve server operating system incidents
- Document system issues and OS errors

Expert User Technical Support*

Expert-to-expert helpdesk support:

- 24 x 7 technical support for priority 1 and 2 incidents
- 8 am to 5 pm technical support for priority 3, 4 and 5 incidents

* An Expert User is defined as someone with in-depth application or system knowledge and a single point of contact for escalating incidents to Company. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage any standard OS security features

Operating System Upgrades

- Periodic next version analysis and recommendations
- Minor version upgrades available by request (Version.x upgrades)
- Major version upgrades that require a full rebuild of the system will be provided on time and materials project basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Out-of-Band Management Access

- Provide Company the ability to access the server over an out-of-band console/lights-out management console with the ability to force a reboot and remotely power on the server

Operating System and Application Software Licensing

- Procure software and licensing for current version of OS, including any user access licensing
- Procure current OS software maintenance where applicable
- End-user access licensing
- Application and database licensing, if applicable

Hardware Maintenance Coverage

- Procurement of hardware maintenance for the duration of the MSA
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Ensure that Company is an authorized caller to maintenance service providers

Hardware Monitoring

- Monitoring of hardware components are outside of the scope of this ItemID

Client Premises Environmentals and Remote Hands

- Where the server is not in a Company data center
    - Client will provide adequate power, environmental, physical security, and network connections.
    - Provide designated on-site data center hands and eyes under the direction of a Company administrator on Company request to execute tasks such as:
        - Rack and connect device
        - Turning server off or on
        - Handle backup tapes
        - Provide accompanied access to the device for maintenance technicians

Virus Protection Software Licensing and Administration (if Client requires Virus Protection)

- Procure virus protection software and licensing and maintenance for current version of OS of the VM
- Manage antivirus software and updates
- Installation of antivirus software

End User Support

- Support of non-expert OS users (Typically refers to non-IT department staff or application end users)

Backup Job Administration and Backup Infrastructure (if server is required to be backed up)

Backup Job Administration

- Administration of server backup jobs
- Installing and maintaining agents
- Backup restores

Backup system to enable backup of data from this server:

- Contracted usage of the Company backup service which includes server backup job management

or

- Backup server and agent licensing with available disk storage and tape media, if required
- Administration of backup system
- Tape storage (if applicable)

601948 Microsoft Azure VM Administration Windows Server

Company's Responsibilities and Included Features

General

Company will provide administration of a virtual machine (VM) running Microsoft Windows Server deployed in Microsoft Azure as described herein.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage standard VM and OS security features
- Manage secure network access to the VM

Network Administration Services

- NIC Administration

VM Administration

- VM resizing
  - Scaling up - make changes as requested by Client via service ticket submission
  - Scaling down make changes as requested by Client via service ticket submission, limited to 1 change per quarter
- Storage Administration
- Availability set Administration
- Boot diagnostics
- VM resource group assignment
- VM tagging

Azure Backup Administration (if server is required to be backed up)

- Administration of VM backup jobs
- Backup restores
- Alert configuration and triage
- Vault configuration for Azure backup
- Administration of backup frequency and retention policies

Operating System Administration

System administration of the server operating system (OS) including:

- OS configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks
- Start and stop services
- Document applicable OS administration procedures and policies

Built in OS Applications Management

Administration of the following built-in OS components that are bundled with the OS:

- Performance monitor
- Device manager
- Windows Update service
- Windows Firewall

The following components are specifically excluded from administration under this ItemID:

- Remote Desktop Services (RDS)
- Licensing/Terminal Server Gateway

SharePoint Services
- Active Directory Services/Application Directory Admin Mode/Active Directory Federation Services
- Server virtualization services
- Application server(s) -IIS/WWW-IIS/FTP-IIS/SMTP
- Certificate Services
- Certification Authority
- DHCP
- DNS
- WINS
- Distributed File System (DFS)
- File system management / DFS replication services
- Windows Deployment Services
- Failover Clustering
- Print Management

Windows Server Monitoring

- Install Company licensed monitoring agents where applicable
- Configure monitoring thresholds and parameters
- Monitor and report key metrics including:
-
    - Disk utilization
    - Processor load
    - Memory usage
    - Core OS services, like:
        - Cryptographic Service
        - Local Session Manager
        - Remote Procedure Call (RPC)
        - Security Accounts Manager
        - Server
        - Task Scheduler
        - Windows Event Log
        - Windows Firewall
        - Windows Time
        - Workstation
    - Client may request application-level services monitoring with notification only. Development of application custom monitoring scripts may incur additional one-time fees, contracted on a separate time and materials project basis
    - Server availability

Windows Server Patch Administration- Level 1 Patch Baseline - Microsoft Security Update

- Monthly review of Microsoft Windows Server security updates
- Company will follow a change control process to include notice submission, approval and application of security updates, as further provided herein

This Level 1 Patch Baseline provides for application of Microsoft security updates for the following components:

- Cumulative security updates for core OS (applies to the latest Windows Server version only)
- Security only updates for core OS (applies to Windows Server versions other than the latest Windows Server version)
- Security only updates for .NET framework
- Therapeutic reboots

Client to provide at a minimum, a four (4) hours monthly patch window for patching plus an additional minimum of one and one-half (1.5) hours for each group of servers rebooted as a group

Client is limited to three (3) patch windows per month across all Windows Servers, unless mutually agreed upon by all Parties

If Client does not provide Company with an opportunity to apply the necessary critical and security updates, and patching is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes and Client may incur additional charges. Client acknowledges and accepts all risk of limiting the Company from applying security updates beyond the above three-month period.

For servers that are normally offline, Company will bring the server online monthly in order to apply OS patches during scheduled patching windows. These servers and their applications must allow for/support this monthly patching window, including bootup and shutdown of the server by both manual and automatic processes. Company understands the desire for certain servers to remain offline; however, Company is not responsible for resource usage costs incurred while the servers are online.

Server Incident Triage and Troubleshooting

- Triage of server OS incidents
- Troubleshoot and work to resolve server OS incidents
- Document system issues and OS errors

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Operating System Upgrades

- Periodic next version analysis and recommendations
- Notifications of upcoming OS End of Life
- Upgrades to a new major version of the OS or embedded OS application are outside of the scope of this ItemID and may be provided on a separate time and materials project basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating System Software Licensing

- Procure OS software and licensing for current version of OS, including any user access licensing

Client Access Licensing

- End-user access licensing of OS or applications, if applicable

Virus Protection Software Licensing and Administration

- Procure virus protection software and licensing and maintenance for current version of OS of the VM
- Manage antivirus software and updates
- Installation of antivirus software

End User Support

- Support of non-expert OS users (typically refers to non-IT department staff or application end users)

Microsoft Azure Subscription

- Azure subscription and resources needed to support Azure VM
- Provide Azure monitoring resources Azure Monitor and Log Analytics for service monitoring
- Provide Company access to Azure Subscriptions and Resource Groups
- Provide Company access to the Azure VM and OS

Azure VM Administration

The following may be provided on a separate time and materials project basis:

- Network Security Group administration
- Region migration
- Maintain VM extensions
- Resource Group Administration

Network Administration Services

The following may be provided on a separate time and materials project basis:

- Load balancer administration
- Firewall administration
- VPN administration
- VNet administration

602064 Microsoft Azure VM Administration - RHEL Linux Server

Company's Responsibilities and Included Features

General

Company will provide administration of a virtual machine (VM) running Red Hat Enterprise Linux (RHEL) deployed in Microsoft Azure as described herein.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage standard VM and OS security features
- Manage secure network access to the VM

Network Administration Services

- NIC Administration

VM Administration

- VM resizing
-
    - Scaling up - make changes as requested by Client via service ticket submission
    - Scaling down make changes as requested by Client via service ticket submission, limited to 1 change per quarter
- Storage Administration
- Availability set Administration
- Boot diagnostics
- VM resource group assignment
- VM tagging

Azure Backup Administration (if server is required to be backed up)

- Administration of VM backup jobs
- Backup restores
- Alert configuration and triage

- Vault configuration for Azure backup
- Administration of backup frequency and retention policies

Operating System Administration

System administration of the server operating system (OS) including:

- OS configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks
- Start and stop services/daemons/processes
- Document applicable OS administration procedures and policies

Built in OS Applications Administration

Administration of the following built-in OS components that may be bundled with the OS:

- SSH
- Firewall configuration
- NIC configuration

Excludes:

- Application server(s) - Examples: Apache/Tomcat(Java)/mySQL/postgresql/FTP
- Certificate services
- Certification authority
- Non-OS file systems replication services
- 3rd party application management
- SElinux
- Server used as Routed Firewall
- Print management
- SAMBA/CIF/Network file management
- SMTP management
- DNS management/BIND
- OS clustering
- GUI/Xserver
- DHCP
- Custom Script/Modules

Linux Server Monitoring

- Install monitoring agents where applicable
- Configure monitoring thresholds and parameters
- Monitor and report key metrics including:
    - Disk utilization
    - Processor load
    - Memory usage
    - Server availability
    - Core OS services including such as:
        - Cron
        - Syslog
        - SSH
        - NTP

Server availability

- Client may request application-level services monitoring with notification only

Linux Server Patch Administration of OS Security Updates

- Monthly review of OS vendor security updates
- Company will follow a change control process to include notice submission, approval and application of security updates, as further provided herein

Client to provide at a minimum, a four (4) hours monthly patch window for patching plus an additional minimum of one and one-half (1.5) hours for each group of servers rebooted as a group

Client is limited to three (3) patch windows per month across all servers, unless mutually agreed upon by all Parties

If Client does not provide Company with an opportunity to apply the necessary security updates, and patching is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes and Client may incur additional charges. Client acknowledges and accepts all risk of limiting the Company from applying security updates beyond the above three-month period.

For servers that are normally offline, Company will bring the server online monthly in order to apply OS patches during scheduled patching windows. These servers and their applications must allow for/support this monthly patching window, including bootup and shutdown of the server by both manual and automatic processes. Company understands the desire for certain servers to remain offline; however, Company is not responsible for resource usage costs incurred while the servers are online.

Server Incident Triage and Troubleshooting

- Triage of server OS incidents
- Troubleshoot and work to resolve server operating system incidents
- Document system issues and OS errors

Expert User Technical Support*

Expert-to-expert helpdesk support:

- 24 x 7 technical support for priority 1 and 2 incidents
- 8 am to 5 pm technical support for priority 3, 4 and 5 incidents

* An Expert User is defined as someone with in-depth application or system knowledge and a single point of contact for escalating incidents to Company. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage any standard OS security features

Operating System Upgrades

- Periodic next version analysis and recommendations
- Minor version upgrades available by request (Version.x upgrades)
- Major version upgrades that require a full rebuild of the system will be provided on time and materials project basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating System and Application Software Licensing

- Procure software and licensing for current version of OS, including any user access licensing
- Procure current OS software maintenance where applicable
- End-user access licensing

- Application and database licensing, if applicable

Virus Protection Software Licensing and Administration (if Client requires Virus Protection)

- Procure virus protection software and licensing and maintenance for current version of OS of the VM
- Manage antivirus software and updates
- Installation of antivirus software

End User Support

- Support of non-expert OS users (Typically refers to non-IT department staff or application end users)

Microsoft Azure Subscription

- Azure subscription and resources needed to support Azure VM
- Provide Azure monitoring resources Azure Monitor and Log Analytics for service monitoring
- Provide Company access to Azure Subscriptions and Resource Groups
- Provide Company access to the Azure VM and OS

Azure VM Administration

The following may be provided on a separate time and materials project basis:

- Network Security Group administration
- Region migration
- Maintain VM extensions
- Resource Group Administration

Network Administration Services

The following may be provided on a separate time and materials project basis:

- Load balancer administration
- Firewall administration
- VPN administration
- VNet administration

602182 SUSE Linux Server Administration - VM

Company's Responsibilities and Included Features

General

Company will provide administration of a SUSE Linux (SUSE) virtual machine (VM) as described herein.

System Administration

System administration of the server operating system (OS) including:

- OS configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks
- Start and stop services/daemons/processes
- Document applicable OS administration procedures and policies

Built in OS Applications Administration

Administration of the following built-in OS components that may be bundled with the OS:

- SSH
- Firewall configuration
- NIC configuration

Excludes:

- Application server(s) - Examples: Apache/Tomcat(Java)/mySQL/postgresql/FTP
- Certificate services
- Certification authority
- Non-OS file systems replication services
- 3rd party application management
- SElinux
- Server used as Routed Firewall
- Print management
- SAMBA/CIF/Network file management
- SMTP management
- DNS management/BIND
- OS clustering
- GUI/Xserver
- DHCP
- Custom Script/Modules

Linux Server Monitoring

- Install monitoring agents where applicable
- Configure monitoring thresholds and parameters
- Monitor and report key metrics including:
    - Cron
    - Syslog
    - SSH
    - NTP
    - Server availability
-
    - Disk utilization
    - Processor load
    - Memory usage
    - Server availability
    - Core OS services including such as:
- Client may request application-level services monitoring with notification only. Development of application custom monitoring scripts may incur additional one-time fees, contracted on a separate time and materials project basis

Linux Server Patch Administration of OS Security Updates

- Monthly review of OS vendor security updates
- Company will follow a change control process to include notice submission, approval and application of security updates, as further provided herein

Client to provide at a minimum, a four (4) hours monthly patch window for patching plus an additional minimum of one and one-half (1.5) hours for each group of servers rebooted as a group

Client is limited to three (3) patch windows per month across all servers, unless mutually agreed upon by all Parties

If Client does not provide Company with an opportunity to apply the necessary security updates, and patching is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes and Client may incur additional charges. Client acknowledges and accepts all risk of limiting the Company from applying security updates beyond the above three-month period.

For servers that are normally offline, Company will bring the server online monthly in order to apply OS patches during scheduled patching windows. These servers and their applications must allow for/support this monthly patching window, including bootup and shutdown of the server by both manual and automatic processes. Company understands the desire for certain servers to remain offline; however, Company is not responsible for resource usage costs incurred while the servers are online.

Server Incident Triage and Troubleshooting

- Triage of server OS incidents
- Troubleshoot and work to resolve server operating system incidents
- Document system issues and OS errors

Expert User Technical Support*

Expert-to-expert helpdesk support:

- 24 x 7 technical support for priority 1 and 2 incidents
- 8 am to 5 pm technical support for priority 3, 4 and 5 incidents

* An Expert User is defined as someone with in-depth application or system knowledge and a single point of contact for escalating incidents to Company. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage any standard OS security features

Operating System Upgrades

- Periodic next version analysis and recommendations
- Minor version upgrades available by request (Version.x upgrades)
- Major version upgrades that require a full rebuild of the system will be provided on time and materials project basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating System and Application Software Licensing

- Procure software and licensing for current version of OS, including any user access licensing
- Procure current OS software maintenance where applicable
- End-user access licensing
- Application and database licensing, if applicable

Virtualization Platform

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide console access to the OS

Virus Protection Software Licensing and Administration (if Client requires Virus Protection)

- Procure virus protection software and licensing and maintenance for current version of OS of the VM
- Manage antivirus software and updates
- Installation of antivirus software

End User Support

- Support of non-expert OS users (Typically refers to non-IT department staff or application end users)

Backup Job Administration and Backup Infrastructure (if server is required to be backed up)

Backup Job Administration

- Administration of server backup jobs
- Installing and maintaining agents
- Backup restores

Backup system to enable backup of data from this server:

- Contracted usage of the Company backup service which includes server backup job management

or

- Backup server and agent licensing with available disk storage and tape media, if required
- Administration of backup system
- Tape storage (if applicable)

602183 Oracle Linux Server Administration - VM

Company's Responsibilities and Included Features

General

Company will provide administration of an Oracle Linux (OL) virtual machine (VM) as described herein.

System Administration

System administration of the server operating system (OS) including:

- OS configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks
- Start and stop services/daemons/processes
- Document applicable OS administration procedures and policies

Built in OS Applications Administration

Administration of the following built-in OS components that may be bundled with the OS:

- SSH
- Firewall configuration
- NIC configuration

Excludes:

- Application server(s) - Examples: Apache/Tomcat(Java)/mySQL/postgresql/FTP
- Certificate services
- Certification authority
- Non-OS file systems replication services
- 3rd party application management
- SElinux
- Server used as Routed Firewall
- Print management
- SAMBA/CIF/Network file management
- SMTP management
- DNS management/BIND

- OS clustering
- GUI/Xserver
- DHCP
- Cron Job creation/modification
- Custom Script/Modules

Linux Server Monitoring

- Install monitoring agents where applicable
- Configure monitoring thresholds and parameters
- Monitor and report key metrics including:
    - Cron
    - Syslog
    - SSH
    - NTP
    - Server availability
-
    - Disk utilization
    - Processor load
    - Memory usage
    - Server availability
    - Core OS services including such as:
- Client may request application-level services monitoring with notification only. Development of application custom monitoring scripts may incur additional one-time fees, contracted on a separate time and materials project basis

Linux Server Patch Administration of OS Security Updates

- Monthly review of OS vendor security updates
- Company will follow a change control process to include notice submission, approval and application of security updates, as further provided herein

Client to provide at a minimum, a four (4) hours monthly patch window for patching plus an additional minimum of one and one-half (1.5) hours for each group of servers rebooted as a group

Client is limited to three (3) patch windows per month across all servers, unless mutually agreed upon by all Parties

If Client does not provide Company with an opportunity to apply the necessary security updates, and patching is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes and Client may incur additional charges. Client acknowledges and accepts all risk of limiting the Company from applying security updates beyond the above three-month period.

For servers that are normally offline, Company will bring the server online monthly in order to apply OS patches during scheduled patching windows. These servers and their applications must allow for/support this monthly patching window, including bootup and shutdown of the server by both manual and automatic processes. Company understands the desire for certain servers to remain offline; however, Company is not responsible for resource usage costs incurred while the servers are online.

Server Incident Triage and Troubleshooting

- Triage of server OS incidents
- Troubleshoot and work to resolve server operating system incidents
- Document system issues and OS errors

Expert User Technical Support*

Expert-to-expert helpdesk support:

- 24 x 7 technical support for priority 1 and 2 incidents

- 8 am to 5 pm technical support for priority 3, 4 and 5 incidents

* An Expert User is defined as someone with in-depth application or system knowledge and a single point of contact for escalating incidents to Company. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage any standard OS security features

Operating System Upgrades

- Periodic next version analysis and recommendations
- Minor version upgrades available by request (Version.x upgrades)
- Major version upgrades that require a full rebuild of the system will be provided on time and materials project basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating System and Application Software Licensing

- Procure software and licensing for current version of OS, including any user access licensing
- Procure current OS software maintenance where applicable
- End-user access licensing
- Application and database licensing, if applicable

Virtualization Platform

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide console access to the OS

Virus Protection Software Licensing and Administration (if Client requires Virus Protection)

- Procure virus protection software and licensing and maintenance for current version of OS of the VM
- Manage antivirus software and updates
- Installation of antivirus software

End User Support

- Support of non-expert OS users (Typically refers to non-IT department staff or application end users)

Backup Job Administration and Backup Infrastructure (if server is required to be backed up)

Backup Job Administration

- Administration of server backup jobs
- Installing and maintaining agents
- Backup restores

Backup system to enable backup of data from this server:

- Contracted usage of the Company backup service which includes server backup job management

or

- Backup server and agent licensing with available disk storage and tape media, if required
- Administration of backup system
- Tape storage (if applicable)

602184 Microsoft Azure VM Administration - SUSE Linux Server

Company's Responsibilities and Included Features

General

Company will provide administration of a virtual machine (VM) running SUSE Linux (SUSE) deployed in Microsoft Azure as described herein.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage standard VM and OS security features
- Manage secure network access to the VM

Network Administration Services

- NIC Administration

VM Administration

- VM resizing
-
    - Scaling up - make changes as requested by Client via service ticket submission
    - Scaling down make changes as requested by Client via service ticket submission, limited to 1 change per quarter
- Storage Administration
- Availability set Administration
- Boot diagnostics
- VM resource group assignment
- VM tagging

Azure Backup Administration (if server is required to be backed up)

- Administration of VM backup jobs
- Backup restores
- Alert configuration and triage
- Vault configuration for Azure backup
- Administration of backup frequency and retention policies

Operating System Administration

System administration of the server operating system (OS) including:

- OS configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks
- Start and stop services/daemons/processes
- Document applicable OS administration procedures and policies

Built in OS Applications Administration

Administration of the following built-in OS components that may be bundled with the OS:

- SSH
- Firewall configuration
- NIC configuration

Excludes:

- Application server(s) - Examples: Apache/Tomcat(Java)/mySQL/postgresql/FTP
- Certificate services
- Certification authority
- Non-OS file systems replication services
- 3rd party application management
- SElinux
- Server used as Routed Firewall
- Print management
- SAMBA/CIF/Network file management
- SMTP management
- DNS management/BIND
- OS clustering
- GUI/Xserver
- DHCP
- Custom Script/Modules

Linux Server Monitoring

- Install monitoring agents where applicable
- Configure monitoring thresholds and parameters
- Monitor and report key metrics including:
-
    - Disk utilization
    - Processor load
    - Memory usage
    - Server availability
    - Core OS services including such as:
    -
        - Cron
        - Syslog
        - SSH
        - NTP
        - Server availability
- Client may request application-level services monitoring with notification only

Linux Server Patch Administration of OS Security Updates

- Monthly review of OS vendor security updates
- Company will follow a change control process to include notice submission, approval and application of security updates, as further provided herein

Client to provide at a minimum, a four (4) hours monthly patch window for patching plus an additional minimum of one and one-half (1.5) hours for each group of servers rebooted as a group

Client is limited to three (3) patch windows per month across all servers, unless mutually agreed upon by all Parties

If Client does not provide Company with an opportunity to apply the necessary security updates, and patching is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes and Client may incur additional charges. Client acknowledges and accepts all risk of limiting the Company from applying security updates beyond the above three-month period.

For servers that are normally offline, Company will bring the server online monthly in order to apply OS patches during scheduled patching windows. These servers and their applications must allow for/support this monthly patching window, including bootup and shutdown of the server by both manual and automatic processes. Company understands the desire for certain servers to remain offline; however, Company is not responsible for resource usage costs incurred while the servers are

online.

Server Incident Triage and Troubleshooting

- Triage of server OS incidents
- Troubleshoot and work to resolve server operating system incidents
- Document system issues and OS errors

Expert User Technical Support*

Expert-to-expert helpdesk support:

- 24 x 7 technical support for priority 1 and 2 incidents
- 8 am to 5 pm technical support for priority 3, 4 and 5 incidents

* An Expert User is defined as someone with in-depth application or system knowledge and a single point of contact for escalating incidents to Company. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage any standard OS security features

Operating System Upgrades

- Periodic next version analysis and recommendations
- Minor version upgrades available by request (Version.x upgrades)
- Major version upgrades that require a full rebuild of the system will be provided on time and materials project basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating System and Application Software Licensing

- Procure software and licensing for current version of OS, including any user access licensing
- Procure current OS software maintenance where applicable
- End-user access licensing
- Application and database licensing, if applicable

Virus Protection Software Licensing and Administration (if Client requires Virus Protection)

- Procure virus protection software and licensing and maintenance for current version of OS of the VM
- Manage antivirus software and updates
- Installation of antivirus software

End User Support

- Support of non-expert OS users (Typically refers to non-IT department staff or application end users)

Microsoft Azure Subscription

- Azure subscription and resources needed to support Azure VM
- Provide Azure monitoring resources Azure Monitor and Log Analytics for service monitoring
- Provide Company access to Azure Subscriptions and Resource Groups
- Provide Company access to the Azure VM and OS

Azure VM Administration

The following may be provided on a separate time and materials project basis:

- Network Security Group administration

- Region migration
- Maintain VM extensions
- Resource Group Administration

Network Administration Services

The following may be provided on a separate time and materials project basis:

- Load balancer administration
- Firewall administration
- VPN administration
- VNet administration

602185 Microsoft Azure VM Administration - Oracle Linux Server

Company's Responsibilities and Included Features

General

Company will provide administration of a virtual machine (VM) running Oracle Linux (OL) deployed in Microsoft Azure as described herein.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage standard VM and OS security features
- Manage secure network access to the VM

Network Administration Services

- NIC Administration

VM Administration

- VM resizing
-
    - Scaling up - make changes as requested by Client via service ticket submission
    - Scaling down make changes as requested by Client via service ticket submission, limited to 1 change per quarter
- Storage Administration
- Availability set Administration
- Boot diagnostics
- VM resource group assignment
- VM tagging

Azure Backup Administration (if server is required to be backed up)

- Administration of VM backup jobs
- Backup restores
- Alert configuration and triage
- Vault configuration for Azure backup
- Administration of backup frequency and retention policies

Operating System Administration

System administration of the server operating system (OS) including:

- OS configuration
- Preventative maintenance
- Emergency maintenance

- Performance tuning
- Server health checks
- Start and stop services/daemons/processes
- Document applicable OS administration procedures and policies

Built in OS Applications Administration

Administration of the following built-in OS components that may be bundled with the OS:

- SSH
- Firewall configuration
- NIC configuration

Excludes:

- Application server(s) - Examples: Apache/Tomcat(Java)/mySQL/postgresql/FTP
- Certificate services
- Certification authority
- Non-OS file systems replication services
- 3rd party application management
- SElinux
- Server used as Routed Firewall
- Print management
- SAMBA/CIF/Network file management
- SMTP management
- DNS management/BIND
- OS clustering
- GUI/Xserver
- DHCP
- Custom Script/Modules

Linux Server Monitoring

- Install monitoring agents where applicable
- Configure monitoring thresholds and parameters
- Monitor and report key metrics including:
    - Disk utilization
    - Processor load
    - Memory usage
    - Server availability
    - Core OS services including such as:
        - Cron
        - Syslog
        - SSH
        - NTP
        - Server availability
- Client may request application-level services monitoring with notification only

Linux Server Patch Administration of OS Security Updates

- Monthly review of OS vendor security updates
- Company will follow a change control process to include notice submission, approval and application of security updates, as further provided herein

Client to provide at a minimum, a four (4) hours monthly patch window for patching plus an additional minimum of one and

one-half (1.5) hours for each group of servers rebooted as a group

Client is limited to three (3) patch windows per month across all servers, unless mutually agreed upon by all Parties

If Client does not provide Company with an opportunity to apply the necessary security updates, and patching is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes and Client may incur additional charges. Client acknowledges and accepts all risk of limiting the Company from applying security updates beyond the above three-month period.

For servers that are normally offline, Company will bring the server online monthly in order to apply OS patches during scheduled patching windows. These servers and their applications must allow for/support this monthly patching window, including bootup and shutdown of the server by both manual and automatic processes. Company understands the desire for certain servers to remain offline; however, Company is not responsible for resource usage costs incurred while the servers are online.

Server Incident Triage and Troubleshooting

- Triage of server OS incidents
- Troubleshoot and work to resolve server operating system incidents
- Document system issues and OS errors

Expert User Technical Support*

Expert-to-expert helpdesk support:

- 24 x 7 technical support for priority 1 and 2 incidents
- 8 am to 5 pm technical support for priority 3, 4 and 5 incidents

* An Expert User is defined as someone with in-depth application or system knowledge and a single point of contact for escalating incidents to Company. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage any standard OS security features

Operating System Upgrades

- Periodic next version analysis and recommendations
- Minor version upgrades available by request (Version.x upgrades)
- Major version upgrades that require a full rebuild of the system will be provided on time and materials project basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating System and Application Software Licensing

- Procure software and licensing for current version of OS, including any user access licensing
- Procure current OS software maintenance where applicable
- End-user access licensing
- Application and database licensing, if applicable

Virus Protection Software Licensing and Administration (if Client requires Virus Protection)

- Procure virus protection software and licensing and maintenance for current version of OS of the VM
- Manage antivirus software and updates
- Installation of antivirus software

End User Support

Support of non-expert OS users (Typically refers to non-IT department staff or application end users)

Microsoft Azure Subscription

- Azure subscription and resources needed to support Azure VM
- Provide Azure monitoring resources Azure Monitor and Log Analytics for service monitoring
- Provide Company access to Azure Subscriptions and Resource Groups
- Provide Company access to the Azure VM and OS

Azure VM Administration

The following may be provided on a separate time and materials project basis:

- Network Security Group administration
- Region migration
- Maintain VM extensions
- Resource Group Administration

Network Administration Services

The following may be provided on a separate time and materials project basis:

- Load balancer administration
- Firewall administration
- VPN administration
- VNet administration

603768 Microsoft Windows Server VM Administration with Disaster Recovery

Company's Responsibilities and Included Features

General

Company shall provide systems administration of a Microsoft Windows Server virtual Machine (VM), with administration of Disaster Recovery services for the purpose of providing service continuity in the event of a failure that prevents the delivery of services from the primary data center.

Replication of the primary VM to the target DR servers is to be provided through the use of hypervisor and requires Client provided hypervisor with replication software or Company contracted replication Service Item which will perform the replication.

Company shall maintain technical Disaster Recovery failover procedures. Change Orders that add to or modify the primary VM or Disaster Recovery environment under Company Disaster Recovery administration will include necessary one-time costs to enhance/update the Disaster Recovery failover procedures.

Primary VM Administration

System Administration

System administration of the server operating system (OS) including:

- OS configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks
- Start and stop services
- Document applicable OS administration procedures and policies

Built in OS Applications Administration

Administration of the following built-in OS components that are bundled with the OS:

- Performance monitor
- Device manager
- Windows Update Service
- Windows Firewall

The following components are specifically excluded from administration under this ItemID:

- Remote Desktop Services (RDS), (formerly known as Terminal Services)
- Licensing/Terminal Server Gateway
- Windows SharePoint Services (WSS)
- Active Directory Services/Application Directory Admin Mode/Active Directory Federation Services
- Server virtualization services
- Application server(s) -IIS/WWW-IIS/FTP-IIS/SMTP
- Certificate Services
- Certification Authority
- DHCP
- DNS
- WINS
- Distributed file system (DFS)
- File system management / DFS replication services
- Windows Deployment Services
- Failover Clustering
- Print Management

Server Backup Job Management

Management of server backup agents and jobs in instances where servers are required by Client to be backed up and are backed up by a Company approved backup environment

- Install local backup software or agent where required
- Configure local backup software or agent where required
- Monitor OS and file system backup job status
- Rectify and resubmit failed backup jobs if appropriate
- Ad hoc backup or restore onto server (limited to 4 restores per year)

Windows Server Monitoring

- Install Company licensed monitoring agents where applicable
- Configure monitoring thresholds and parameters
- Monitor and report key metrics including:
    - Disk utilization
    - Processor load
    - Memory usage
    - Core OS services including such as:
        - Cryptographic Service
        - Local Session Manager
        - Remote Procedure Call (RPC)
        - Security Accounts Manager
        - Server
        - Task Scheduler
        - Windows Event Log
        - Windows Firewall
        - Windows Time

        - Workstation
    - Client may request application-level services monitoring with notification only. Development of application custom monitoring scripts may incur additional one-time fees, contracted on a separate time and materials project basis
    - Server availability

Windows Server Patch Management - Level 1 Patch Baseline - Microsoft Critical and Security Update

- Monthly review of Microsoft Windows Server security updates
- Company will follow a change control process to include notice submission, approval and application of security updates, as further provided herein

This Level 1 Patch Baseline provides for application of Microsoft security updates for the following components:

- Cumulative security patching for core OS (applies to the latest Windows Server version only)
- Security only updates for core OS (applies to Windows Server versions other than the latest Windows Server version)
- Security only updates for .NET framework
- Therapeutic reboots

Client to provide at a minimum, a four (4) hours monthly patch window for patching plus an additional minimum of one and one-half (1.5) hours for each group of servers rebooted as a group

Client is limited to three (3) patch windows per month across all Windows Servers, unless mutually agreed upon by all Parties

If Client does not provide Company with an opportunity to apply the necessary critical and security patches, and patching is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes and Client may incur additional charges. Client acknowledges and accepts the risk of limiting the Company from applying critical and security patches beyond the above three-month period.

Server Incident Triage and Troubleshooting

- Triage of server OS incidents
- Troubleshoot and work to resolve server operating system incidents
- Document system issues and OS errors

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and a single point of contact for escalating incidents to Company. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage standard local OS security features

Operating System Upgrades

- Periodic next version analysis and recommendations
- Notifications of upcoming OS End of Life
- Upgrades to a new major version of the OS or embedded OS application are outside of the scope of this ItemID and may be provided on a separate time and materials project basis

Disaster Recovery Administration

Recovery Point Objective (RPO) Management

- RPO is defined as the maximum amount of data that will be unavailable in the DR VM in terms of time, backward from the point of disaster.
- RPO will be limited by the network bandwidth available for the replication of data from the primary VM to the target DR data center and the rate of change on the primary VM. RPO will be monitored and managed for variance outside the reasonably acceptable norms for the Client s specific environments.

Recovery Time Objective (RTO) Management

- RTO is defined as the time from when a disaster is declared until the target DR VM is operational and available on the DR network
- An RTO will be set after deployment of the DR environment and initial, successful failover test has been conducted

Application Failover Testing

- One (1) annual failover test for this service will be conducted in collaboration with the Client.
- The duration of the annual DR Test will be limited to 48 hours, with a Company s level of effort limited to 12 hours of engineer/administrator time
- DR testing will be conducted in an isolated DR test network without stopping source environments
- During failover testing the Disaster Recovery systems may not be receiving updated replication data from the production system thus the RPO may not be met, and should a disaster occur during a test the recovery data will be as old as the data was when testing began.

Application Failover Services

- On declaration of a disaster, Company will perform the steps necessary to restart and validate the VM on the target DR server and make it the primary VM, operational and accessible on the DR network as defined in the Disaster Recovery Failover Procedures.
- During the period that the target DR VM is acting as the primary VM, administration of the VM will be as per the administrative, support, backup, and monitoring services as defined for the primary VM.

Application Failback Services

- When the ability to provide services from the Primary Site is restored, Company will schedule, in collaboration with the Client, and initiate failback to the primary environment as documented in the Disaster Recovery Failover Procedures, and return service back to the Primary Site.
- Application Failback Services will be provided on a project, time and material basis

Replication Management

- Configuration of replication policies
- Monitoring of replication services
- Diagnosis of replication incidents
- Troubleshooting of replication incidents
- Engagement of software providers Help Desk support

Disaster Recovery Replication Incident Triage and Troubleshooting

- Triage of VM replication incidents
- Troubleshoot and work to resolve replication incidents
- Where necessary Company will engage and log service requests with the replication software vendor for support to rectify software issues
- Provide client with updates
- Document user issues and system errors

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Operating System Software Licensing

- Procure OS software and licensing for current version of OS, including any user access licensing
- Provide software media for installation
- Procure current software maintenance where applicable

Servers deployed on Company's public cloud, VPC or FLEX platforms include a license for any supported version of Microsoft Server

Virus Protection Software Licensing and Management

- Procure virus protection software and licensing and maintenance for current version of operating system of the VM
- Manage antivirus software and updates
- Installation of antivirus software

Virtualization Platform

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software with replication capabilities on which the VM being managed is run
- Manage virtualization platform
- Provide console access to the OS

Client Access Licensing

- End-user access licensing of OS or applications, if applicable

End User Support

- Support of non-expert OS users (Typically refers to non-IT department staff or application end users)

Backup Job Administration and Backup Infrastructure (Tape or Disk Based) (if server is required to be backed up)

Backup Job Administration

- Administration of server backup jobs
- Installing and maintaining agents
- Backup restores

Backup system to enable backup of data from this server to tape or disk:

- Contracted usage of the Company backup service which includes server backup job management

or

- Backup server and agent licensing, with available disk storage and tape media if required
- Management of backup system
- Tape storage (on-site or off-site, if applicable)

Business Continuity / Disaster Recovery Plan

A strategic and tactical plan that describes the roles, responsibilities, actions and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation

604542 Oracle Linux Virtualization Manager Disaster Recovery Administration - Per VM

Company's Responsibilities and Included Features

General

Oracle Linux Virtualization Manager (OLVM) supports active-passive disaster recovery to ensure that environments can recover

when a site outage occurs. The solution support two sites and require replicated storage.

Active-passive disaster recovery is a site-to-site failover solution. Two separate OLVM environments are configured: The active primary environment and the passive secondary (backup) environment. With the active-passive disaster recovery, Company will manually execute failover and failback.

Failover is achieved by configuring a secondary site with:

- An active OLVM Engine.
- A data center and clusters (Bare Metal Nodes).
- Networks with the same general connectivity as the primary site.
- Active hosts capable of running critical virtual machines after failover.
- Data replication is facilitated by Volume Group Replication, using Asynchronous replication schedules, and support a Recovery Point Objective (RPO) no faster than 1 hour.

The failover and failback processes are executed manually using Ansible playbooks that map entities between the sites and manage the failover and failback processes. The mapping file instructs the OLVM components where to failover or failback to.

Company shall provide Disaster Recovery (DR) administration of OLVM recovery Volume Group (storage) Replication of the virtual Servers. Company shall perform the following:

- Creation of mapping file.
- Creation and management of playbooks (failover and failback).
- Replication and recovery service as part of a DR plan. This service solely applies to:
    - Maintaining the configuration of the recovery policies used to define replication of Virtual Machine (VM)
    - Maintaining the plan for recovery from the primary data center to the disaster recovery data center
    - Providing the technical administration of DR tests and/or
    - Conducting a DR failover in the case a DR event is declared.
- Requires: ItemID 604543 Oracle Linux Virtualization Manager Disaster Recovery Administration (per VM) setup.

Replication and Recovery Plan Management

- Configuration of replication policies.
- Maintain DR test and failover recovery plans for the virtual servers and Company sdata center network reconfiguration for DR testing or DR failover.
- Monitoring of replication services.
- Triage and troubleshooting of replication incidents.
- Engagement of replication software providers help desk support

Replication Point Objective (RPO) Management

- RPO is defined as the maximum amount of data that will be unavailable in the DR system in terms of time, backward from the point of disaster.
- RPO will be limited by the network bandwidth available for replication of data from the primary servers to the target DR data center and the rate of change on the primary servers. RPO will be monitored and managed for variance outside the reasonably acceptable norms for the Client s specific environments.Configuration of replication policies.

Recovery Time Objective (RTO) Management

RTO is defined as the time from when a disaster is declared until the target DR server operating system is operational and available on the DR network. An RTO will be set after deployment of the DR environment and an initial failover test has been conducted.

Server Failover Testing

- One (1) annual failover test for this service will be conducted in collaboration with the Client.
- The duration of the annual DR test will be limited to 48 hours, with a Company s level of effort limited to 3 hours of engineer/administrator time per VM.

DR testing will be conducted in an isolated DR test network without stopping source environments.

- DR testing by Company is limited to ensuring that the VM boots up in the sequence defined in the recovery/test plan.

Server Failover Services

- On declaration of a disaster, Company will undertake to activate the target DR servers and make them the active servers, operational and accessible on the DR network as defined in the DR failover procedures.
- Rerouting network traffic.
- During the period that the target DR server is acting as the active server, administration of the server will be as per the administrative, support, backup and monitoring services as defined for the primary server.

Server Failback Services

- When the ability to provide services from the primary server is restored, Company will initiate failback to the primary server as documented in the DR failover procedures, and in collaboration with the Client, schedule and return service back to the primary site.

- Reestablishment of replication back to the target DR server will then be activated and services will return back to its normal operational mode.
  Server Failback Services will be provided on a project, time, and material basis

The server failback process is a disruptive process that will create an outage. Client should plan for down time for this process. Company will assist Client in planning for this procedure.

Expert User Technical Support:

Technical support may only be requested by a Client s Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of Client s impact and urgency as further provided in the Company s Customer Operations Handbook.

* An Expert User is defined as someone with an in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Disaster Recovery Replication Software Licensing :

Procurement of current software maintenance, where applicable, are included within Oracle Linux Virtualization Manager. ReliaCloud EDGE solutions in support of bare metal hypervisors, such as OLVM, will include volume group replication utilities. OLVM includes software to script the recovery.

Business Continuity / Disaster Recovery Plan

A strategic and tactical plan that describes the roles, responsibilities, actions, and the parties responsible for carrying them out, in response to a series of identified risks, with the objective of restoring normal business operation.

Disaster Recovery:

- Declaration of a disaster to initiate a recovery plan. The need to declare a disaster should be discussed with Company declaring the disaster to ensure that this is the best course of action.
- Executing any/all recovery plan actions needed within the operating system, database or applications
- Coordination with WAN circuit providers to re-route WAN traffic during a DR eventClient is responsible for all disaster recovery solutions and associated services.

Disaster Recovery:

Inform Company of changes to:

- DR recovery retention window.
- Server startup sequencing and startup delay.
- Network mapping.
- Server re-IP plan (if applicable).

Virtualization Platform:

- Virtualization platform with sufficient capacity in the source (production) and target (DR) datacenters.
- Capacity must include the necessary capacity for the DR replication software servers/virtual appliances.
- Virtualization platform host hardware (Disk, CPU and RAM).
- Virtualization software on which the virtual machine being managed is run.
- Management of virtualization platform.

Replication Network:

- A network connection between the Primary and Recovery Sites with sufficient bandwidth to accommodate the RPO requirements.

Operating System, Database network and Applications and Client-Side DR Configuration and Testing

- Maintain DR test and failover procedures for all operating systems, databases, and applications existing on the servers included in the DR plan.
- Operating system, database and application management, and reconfiguration during DR testing or failover.
- Configurations of end-user devices and/or Client infrastructure that are required to allow end-users to access the environment.
- Conducting functional and data validation testing during server failover testing.

604545 Oracle Linux Virtualization Manager - Management

Company's Responsibilities and Included Features

System Administration

System administration of Oracle Linux Virtualization Manager ("Hypervisor) includes:

- Hypervisor configuration
- Hypervisor monitoring
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks
- Virtual machine provisioning
- Management of Oracle VM server through the Virtualization Manager
- Management of Oracle VM Manager
- Management of iSCSI attached storage and volume group replication if applicable

Note: The minimum cluster size must include at least two (2) Hypervisors to be eligible for Company management.

Hypervisor System Upgrade, Update and Patch Management

- Periodic review and application of Hypervisor patches or updates.
- Application of patches and minor release updates.
- A minor release is a release of a product that does not add significant new features or content and is primarily a bundle of performance or bug fix patches.
- Major release (x and .x) upgrades will be provided on a time and material basis contracted under a separate Statement of Work.

- Client must provide the Company an opportunity to patch or deploy patches and minor updates to the environment within 90 days of Company notifying the Client of the need to patch or update the environment; otherwise any SLAs on the environment or systems reliant on this service will be waived.
- Required compute and storage hardware upgrades may necessitate major or minor release updates to the Hypervisor.

Server Incident Triage and Troubleshooting

- Triage of server hardware or Hypervisor system incidents
- Troubleshooting of server hardware or Hypervisor system incidents
- Document incidents and Hypervisor system errors

Hardware Maintenance Management

- Manage hardware replacement and or repair with hardware vendor
- Perform analysis of any hardware additions or upgrades
- Apply hardware BIOS updates as necessary

Expert User Technical Support:

Technical support may only be requested by a Client s Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of Client s impact and urgency as further provided in the Company s Customer Operations Handbook.

* An Expert User is defined as someone with an in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Hypervisor System Software Licensing:

- Procurement of software and licensing for current version of hypervisor, including any user access licensing where applicable
- Providing software media for installation
- Procurement of current software maintenance where applicable

Third Party Oracle VM Utilities and Applications

- Management of third-party Hypervisor enhancement tools, utilities or applications

Business Continuity / Disaster Recovery Plan:

- Client is responsible for all disaster recovery solutions and associated services.
- Client s business continuity plan(s) and disaster recovery plan(s) are Client s responsibilities and are out of scope for this engagement.

611511 Microsoft Azure VM Administration - Ubuntu Linux Server

Company's Responsibilities and Included Features

General

Company will provide administration of a virtual machine (VM) running Ubuntu (open-source) deployed in Microsoft Azure as described herein.

Ubuntu administration will be provided on a commercially reasonable basis. Ubuntu is an open-source operating system and is

inherently subject to potential limitations including, but not limited to, the ability for Company s tools to properly support it, the availability of vulnerability updates, and no vendor support. Strong consideration should be given prior to using this OS in production. For the avoidance of doubt, no protections set forth under the Microsoft Customer Agreement are afforded for the services described herein. Company will provide administration of a virtual machine (VM) running CentOS Linux (CentOS) deployed in Microsoft Azure as described herein.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage standard VM and OS security features
- Manage secure network access to the VM

Network Administration Services

- NIC Administration

VM Administration

- VM resizing
-
    - Scaling up - make changes as requested by Client via service ticket submission
    - Scaling down make changes as requested by Client via service ticket submission, limited to 1 change per quarter
- Storage Administration
- Availability set Administration
- Boot diagnostics
- VM resource group assignment
- VM tagging

Azure Backup Administration (if server is required to be backed up)

- Administration of VM backup jobs
- Backup restores
- Alert configuration and triage
- Vault configuration for Azure backup
- Administration of backup frequency and retention policies

Operating System Administration

System administration of the server operating system (OS) including:

- OS configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks
- Start and stop services/daemons/processes
- Document applicable OS administration procedures and policies

Built in OS Applications Administration

Administration of the following built-in OS components that may be bundled with the OS:

- SSH
- Firewall configuration
- NIC configuration

Excludes:

- Application server(s) - Examples: Apache/Tomcat(Java)/mySQL/postgresql/FTP

- Certificate services
- Certification authority
- Non-OS file systems replication services
- 3rd party application management
- SElinux
- AppArmor
- SNAP
- Server used as Routed Firewall
- Print management
- SAMBA/CIF/Network file management
- SMTP management
- DNS management/BIND
- OS clustering
- GUI/Xserver
- DHCP
- Custom Script/Modules

Linux Server Monitoring

- Install monitoring agents where applicable
- Configure monitoring thresholds and parameters
- Monitor and report key metrics including:
    - Disk utilization
    - Processor load
    - Memory usage
    - Server availability
    - Core OS services including such as:
        - Cron
        - Syslog
        - SSH
        - NTP
        - Server availability
- Client may request application-level services monitoring with notification only

Linux Server Patch Administration of OS Security Updates

- Monthly review of OS vendor security updates
- Company will follow a change control process to include notice submission, approval and application of security updates, as further provided herein

Client to provide at a minimum, a four (4) hours monthly patch window for patching plus an additional minimum of one and one-half (1.5) hours for each group of servers rebooted as a group

Client is limited to three (3) patch windows per month across all servers, unless mutually agreed upon by all Parties

If Client does not provide Company with an opportunity to apply the necessary security updates, and patching is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes and Client may incur additional charges. Client acknowledges and accepts all risk of limiting the Company from applying security updates beyond the above three-month period.

For servers that are normally offline, Company will bring the server online monthly in order to apply OS patches during scheduled patching windows. These servers and their applications must allow for/support this monthly patching window, including bootup and shutdown of the server by both manual and automatic processes. Company understands the desire for certain servers to remain offline; however, Company is not responsible for resource usage costs incurred while the servers are online.

Server Incident Triage and Troubleshooting

- Triage of server OS incidents
- Troubleshoot and work to resolve server operating system incidents
- Document system issues and OS errors

Expert User Technical Support*

Expert-to-expert helpdesk support:

- 24 x 7 technical support for priority 1 and 2 incidents
- 8 am to 5 pm technical support for priority 3, 4 and 5 incidents

* An Expert User is defined as someone with in-depth application or system knowledge and a single point of contact for escalating incidents to Company. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage any standard OS security features

Operating System Upgrades

- Periodic next version analysis and recommendations
- Minor version upgrades available by request (Version.x upgrades)
- Major version upgrades that require a full rebuild of the system will be provided on time and materials project basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Ubuntu Pro

- Ubuntu Pro is a distinct version of Ubuntu and not covered under this management item

Operating System and Application Software Licensing

- Procure software and licensing for current version of OS, including any user access licensing
- Procure current OS software maintenance where applicable
- End-user access licensing
- Application and database licensing, if applicable

Virus Protection Software Licensing and Administration (if Client requires Virus Protection)

- Procure virus protection software and licensing and maintenance for current version of OS of the VM
- Manage antivirus software and updates
- Installation of antivirus software

End User Support

- Support of non-expert OS users (Typically refers to non-IT department staff or application end users)

Microsoft Azure Subscription

- Azure subscription and resources needed to support Azure VM
- Provide Azure monitoring resources Azure Monitor and Log Analytics for service monitoring
- Provide Company access to Azure Subscriptions and Resource Groups
- Provide Company access to the Azure VM and OS

Azure VM Administration

The following may be provided on a separate time and materials project basis:

- Network Security Group administration

- Region migration
- Maintain VM extensions
- Resource Group Administration

Network Administration Services

The following may be provided on a separate time and materials project basis:

- Load balancer administration
- Firewall administration
- VPN administration
- VNet administration

611704 Ubuntu Linux Server Administration - VM

Company's Responsibilities and Included Features

General

Company will provide administration of a virtual machine (VM) running Ubuntu (open-source) as described herein.

Ubuntu administration will be provided on a commercially reasonable basis. Ubuntu is an open-source operating system and is inherently subject to potential limitations including, but not limited to, the ability for Company s tools to properly support it, the availability of vulnerability updates, and no vendor support. Strong consideration should be given prior to using this OS in production.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage standard VM and OS security features

Network Administration Services

- NIC Administration

Backup Administration (if server is required to be backed up)

- Administration of VM backup jobs
- Backup restores
- Alert configuration and triage
- Vault configuration for Azure backup
- Administration of backup frequency and retention policies

Operating System Administration

System administration of the server operating system (OS) including:

- OS configuration
- Preventative maintenance
- Emergency maintenance
- Performance tuning
- Server health checks
- Start and stop services/daemons/processes
- Document applicable OS administration procedures and policies

Built in OS Applications Administration

Administration of the following built-in OS components that may be bundled with the OS:

- SSH

- Firewall configuration
- NIC configuration

Excludes:

- Application server(s) - Examples: Apache/Tomcat(Java)/mySQL/postgresql/FTP
- Certificate services
- Certification authority
- Non-OS file systems replication services
- 3rd party application management
- SElinux
- AppArmor
- SNAP
- Server used as Routed Firewall
- Print management
- SAMBA/CIF/Network file management
- SMTP management
- DNS management/BIND
- OS clustering
- GUI/Xserver
- DHCP
- Custom Script/Modules

Linux Server Monitoring

- Install monitoring agents where applicable
- Configure monitoring thresholds and parameters
- Monitor and report key metrics including:
    - Disk utilization
    - Processor load
    - Memory usage
    - Server availability
    - Core OS services including such as:
        - Cron
        - Syslog
        - SSH
        - NTP
        - Server availability
- Client may request application-level services monitoring with notification only

Linux Server Patch Administration of OS Security Updates

- Monthly review of OS vendor security updates
- Company will follow a change control process to include notice submission, approval and application of security updates, as further provided herein

Client to provide at a minimum, a four (4) hours monthly patch window for patching plus an additional minimum of one and one-half (1.5) hours for each group of servers rebooted as a group

Client is limited to three (3) patch windows per month across all servers, unless mutually agreed upon by all Parties

If Client does not provide Company with an opportunity to apply the necessary security updates, and patching is delayed by more than three (3) months, a catch-up patching process will be applied at the time patching resumes and Client may incur additional charges. Client acknowledges and accepts all risk of limiting the Company from applying security updates beyond the above three-month period.

For servers that are normally offline, Company will bring the server online monthly in order to apply OS patches during

scheduled patching windows. These servers and their applications must allow for/support this monthly patching window, including bootup and shutdown of the server by both manual and automatic processes. Company understands the desire for certain servers to remain offline; however, Company is not responsible for resource usage costs incurred while the servers are online.

Server Incident Triage and Troubleshooting

- Triage of server OS incidents
- Troubleshoot and work to resolve server operating system incidents
- Document system issues and OS errors

Expert User Technical Support*

Expert-to-expert helpdesk support:

- 24 x 7 technical support for priority 1 and 2 incidents
- 8 am to 5 pm technical support for priority 3, 4 and 5 incidents

* An Expert User is defined as someone with in-depth application or system knowledge and a single point of contact for escalating incidents to Company. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Security Administration Services

- Provide and maintain OS local user security and permissions
- Manage any standard OS security features

Operating System Upgrades

- Periodic next version analysis and recommendations
- Minor version upgrades available by request (Version.x upgrades)
- Major version upgrades that require a full rebuild of the system will be provided on time and materials project basis

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Ubuntu Pro

- Ubuntu Pro is a distinct version of Ubuntu and not covered under this management item

Operating System and Application Software Licensing

- Procure software and licensing for current version of OS, including any user access licensing
- Procure current OS software maintenance where applicable
- End-user access licensing
- Application and database licensing, if applicable

Virtualization Platform

- Server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide console access to the OS

Virus Protection Software Licensing and Administration (if Client requires Virus Protection)

- Procure virus protection software and licensing and maintenance for current version of OS of the VM
- Manage antivirus software and updates
- Installation of antivirus software

End User Support

- Support of non-expert OS users (Typically refers to non-IT department staff or application end users)

Network Administration Services

The following may be provided on a separate time and materials project basis:

- Load balancer administration
- Firewall administration
- VPN administration
- VNet administration

Backup Job Administration and Backup Infrastructure (if server is required to be backed up)

Backup Job Administration

- Administration of server backup jobs
- Installing and maintaining agents
- Backup restores

Backup system to enable backup of data frm this server:

- Backup server and agent licensing with available disk storage and tape media, if required
- Contracted usage of the Company backup service which includes server backup job management

or

- Administration of backup system
- Tape storage (if applicable)

Category: Managed Storage

601791 Nutanix Files Management - AOS Cluster

Definitions

AOS: Nutanix Acropolis Operating System is Hyper-Converged Infrastructure (HCI) management software that operates the merger of compute, storage, networking and virtualization services

AHV: Nutanix Acropolis Hypervisor

VMware ESXi: VMware's hypervisor platform

Cluster: A logical grouping of Nodes and software to form an IT services entity, generally for the purposes of serving storage, server, and desktop virtualization services

File Server Virtual Machine (FSVM): A virtual machine that runs as part of the Nutanix Files file server service.

ICAP: Internet Content Adaptation Protocol (ICAP) is a lightweight protocol designed to offload processing of Internet-based content to dedicated servers. The goal of ICAP, a lightweight HTTP-based RPC protocol, is to offload tasks like antivirus scanning onto specialized servers to increase network throughput.

Node: A discrete unit of IT infrastructure (CPU, memory, and storage) that participates within a hyper-converged Cluster

Nutanix Files: A software-defined scale-out file storage solution designed to address a wide range of use cases, including but not limited to, support for Linux and Windows home directories, user profiles and department shares.

SMB: Server Message Block, is a network protocol used by Windows-based computers that allows systems within the same network to share files.

Company's Responsibilities and Included Features

Nutanix Files Management AOS Cluster provides OneNeck management services for Nutanix Files (Files) running within a mixed purpose (virtualization services and Files) AOS Cluster running either AHV or VMware ESXi.

Files administration is quantified as per FSVM that participates within the Cluster delivering Files services.

Nutanix Files Administration

Company will support administration of the following functions:

- File Server Management
  - Creating a file server
  - Maintain the Files Cluster
  - File server cloning
  - Encryption settings
  - Antivirus (AV) scanning (SMB Only)
  - Provide recommendations on File Server Virtual Machines (FSVMs) infrastructure sizing including storage requirements based upon workload.
- Files Optimization
  - Performance optimization
  - File system compression
- Share and Export Management
  - Creating file shares
  - Creating exports
  - Multiprotocol support
- Domain Configuration Management
  - Domain joining
  - Updating Domain Name System (DNS) entries
  - Disjoint domain management
- Directory and User Management
  - Updating Files directory services
  - Management of user mappings
  - Managing user roles
  - Management of user quotas
- Data Recovery Management
  - Management of protection domain and snapshot schedule
  - Support for Files asynchronous replication with a minimum 1-hour recovery point objective
  - Upon Client request, activation of disaster recovery of File Server Virtual Machines (FSVMs)
  - Configuration for high availability of FSVMs
  - Configuration of self-service restore (SSR) and snapshot schedule parameters

Nutanix Files analytics is not within scope of this ItemID. Files analytics support is available under a separate ItemID.

Files Triage and Troubleshooting

- Triage of Files system incidents
- Troubleshoot and work to resolve Files system incidents
- Document Files system issues and errors

Files Patching, Updates and Upgrades

- Periodic reviews of critical patches
- Up to quarterly routine review same-version patch analysis
- Manage change order process including notice submission, approval and application of updates, patches and upgrades
- Application of updates and patches during Client approved maintenance windows
- Periodic upgrades to the AOS software (including major upgrades) will be conducted at Company s discretion and in

accordance with industry best practices during Client approved maintenance windows

If Client does not provide Company with a maintenance window to apply updates, patches, and upgrades within a commercially reasonable timeframe based on the severity of the update, upgrade or patch, Client waives any and all claims against Company which arise directly or indirectly from such failure to update, upgrade or patch, and any applicable service level agreements will be suspended until such time as patching, updating and upgrades are up to date. If patching, updating or upgrading is delayed by more than three (3) months, a catch-up process will be applied at the time patching, updating or upgrading resumes, and Client will be invoiced on a time and materials basis for such catch-up services. Client acknowledges and accepts all risk relating to failure to provide maintenance windows for updates, upgrades and/or patches.

Co-administration

Company is providing managed Services on a virtualization platform with an end-user experience making certain self-service features available to Client, including:

- Ability to login into Prism and general visibility into the Cluster metrics and configuration settings such as:
  - Files dashboard
  - File Server alerts and notifications
  - File Server events
- Self-service management
  - Self-service File restoration
  - Execute snapshots and restorations

Company SLA obligations will not apply to incidents caused by Client co-administration activities. Company remediation of Client caused co-administration activities will be charged to Client on time and materials basis.

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

General Requirements

- Provide virtualizing resources to meet or exceed the Nutanix Files infrastructure specifications.
  - Minimum virtualized resources necessary to run the Nutanix Files are as follows per FSVM
    - 4 vCPU
    - 12 GiB memory
    - 3 FSVMs for scale out and fault-tolerance
    - N + 1 available IP addresses for the number of Nodes (N)
    - Directory services for user authentication such as Microsoft Active Directory or LDAP.
    - In Cluster storage network and associated hardware for Files Storage
- Manage end user Files share access management and usage
- Client required to contract with Company for Nutanix AOS Base Features Management
- For anti-virus scanning support, provide ICAP compatible anti-virus software
- Remediate Company identified platform deployment issues prior to Company taking ownership of the platform administration
- Migration of Files data onto and off of the Cluster

- Provide VM resources within the Cluster for Company s operating systems and applications that are used to manage the Client s environment (Management VMs)
- Open necessary network and firewall ports to provide Company access to Management VMs
- Provide VPN termination point for Company to access Client s environment

Hardware and Software Licensing and Maintenance Coverage

- Procure Files software licensing, also available from Company under a separate ItemID.
- Procure all application licensing including but not limited to the hypervisor and VM operating systems
- Procure and maintain hardware and software maintenance for the duration of the SOW
- Provide contract numbers and phone numbers for applicable hardware and software maintenance service providers
- Ensure that Company is an authorized caller to maintenance service providers

Client Premises Remote Hands

- Where the Node is not in a Company data center, provide a designated on-site resource to do the following on Company request
  - Rack and connect device
  - Handle backup tapes
  - Provide accompanied access to the device for maintenance technicians
  - Provide ad hoc on-site non-technical hand and eyes support under the direction of a Company administrator to assist in physical device management

604377 Microsoft Azure Files Share Administration

Company's Responsibilities and Included Features

This service is sized based upon storage consumed by Azure Files per Azure region and subscription. Storage is consumed in 1TB increments.

Azure File Shares Administration

- Add, change, delete Azure Files Shares (AFS)
- Administration of AFS backups using Azure backup, including restores of data from backup, if Client requires backups
- Azure files storage account administration (for Azure Files)
- File share quota administration
- Directory administrator permission management
- File share options configuration
- Manage encryption configuration
- Snapshot administration
- Private endpoint management
- Optional: DNS namespace, Azure AD
- Azure Monitor monitoring for Azure Files if subscribed to by the Client

Incident Triage and Troubleshooting

- Triage of AFS system incidents
- Troubleshooting and working to resolve AFS system incidents
- Troubleshooting and working to resolve AFS permissions and access issues
- Where necessary Company will engage and log service requests with Microsoft to rectify issues
- Provide client with updates
- Document user issues and system errors

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, or Client help desk available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents

- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Microsoft CSP Subscription and Infrastructure

- Microsoft subscription to AFS through Company's CSP program
- Provide Company with an Azure VM with access to each AFS for AFS administration

Shares and Files Migration (this can be provided on a time and materials project basis)

- Migration of files into or out of AFS
- Data reorganization

Data, Permission and Access Management

- Management of access and permissions to file shares, folders, and files
- Host or network-based access control
- User drive and share mapping
- Data management
- Name resolution record management

Protection and Auditing

- File level auditing
- Anti-virus protection
- Share, folder, file level reporting
- Data synchronization
- Regional availability administration

End User Support

- Support of non-expert users (typically refers to non-IT department staff or application end users)

Out of Scope Notes

- Management of storage accounts not solely for the purpose of Azure Files

Category: Management Infrastructure

500159 Remote Management Infrastructure (1-24 devices)

Company's Responsibilities and Included Features

Heading 1

The Remote Management Infrastructure (1-24 devices) provides the necessary infrastructure to facilitate secure, remotely managed services for environments containing less than 25 contracted service entities (devices). Company will deploy and manage the IPSec VPN tunnel which connects the Client's hub location to our Network Operations center (NOC). The IPSec VPN tunnel will be initiated from a Client dedicated firewall instance at Company and will terminate on Client provided infrastructure at the Client's hub location.

- Provide connectivity via IPSec encrypted tunnel from Company to one Client site

- Provide terminating infrastructure and connectivity services at Company Network Operations Center
- Dedicated security service instance (context) specifically for use with remote managed services
- Highly available redundant hardware
- Maintaining firewall operation including current and best supported service version
- Defining and applying security best practices
- All service context configuration activities, including configuration updates and port openings/closures
- Provide Client with a service specific list of port opening requirements to facilitate management services per technology under contract
- Notify Client of IPSec VPN tunnel connectivity issues
- Monitor, maintain, and manage the IPSec VPN tunnel between service locations

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide end tunnel termination equipment on Client premise (Cisco preferred)
- Configure tunnel endpoint
- Notify Company of any service requirements, changes or modifications
- Provide Internet services at hub location
- Allow for specific firewall port openings provided by Company to facilitate management service

500164 Remote Management Infrastructure (25+ devices) - virtual appliance

Company's Responsibilities and Included Features

The Remote Management Infrastructure (25+ devices)

- Virtual appliance provides the necessary infrastructure to facilitate secure, remotely managed services for environments containing 25 or greater contracted service entities (devices). Company will provide a virtual Management Appliances to deployed within a secured segment of the Client's network.
- Provide virtual management appliances (OVA template) for deployment in Client's VMware cluster environment
- Advise Client on logical location and placement of management appliance Company will deploy and manage the IPSec VPN tunnel which connects the Client's hub location to our Network Operations center (NOC). The IPSec VPN tunnel will be initiated from a Client dedicated firewall instance at Company and will terminate on Client provided infrastructure at the Client's hub location
- Provide secure connectivity via IPSec encrypted tunnel from Company to one Client site
- Provide terminating infrastructure and connectivity services at Company Network Operations Center
- Dedicated security service instance (context) specifically for use with remote managed services
- Highly available redundant hardware
- Maintaining firewall operation including current and best supported service version
- Defining and applying security best practices.
- All service context configuration activities, including configuration updates and port openings/closures
- Provide Client with a service specific list of port opening requirements to facilitate management services per technology under contract
- Notify Client of IPSec VPN tunnel or Management Appliance connectivity issues
- Monitor, Maintain, and Manage, virtual management appliances
- Monitor, Maintain, and Manage the IPSec VPN tunnel between service locations

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Provide end tunnel termination equipment on Client premise (Cisco preferred)
- Configure tunnel endpoint
- Notify Company of any service requirements, changes or modifications

- Provisioning of virtual appliance from provided OVA template with the following resources:
  - 1 vCPU
  - 2GB RAM
  - 50GB disk
  - Provide a secured network segment, behind a firewall or router
  - Provide 1 private IP addresses per appliance
  - Provide a secured network segment behind a firewall or router
  - Provide Internet Services at hub location
  - Provide 1 private IP address per appliance
  - Allow for specific firewall port openings provided by Company to facilitate management services

600251 Remote Management Infrastructure for Azure (25+ devices)

Company's Responsibilities and Included Features

Secure connectivity from the Company Network Operations center (NOC) to the Client s Azure environment is required for Company to manage or monitor Client s Azure resources.

A Remote Management Virtual Appliance (RMVA) provides the necessary infrastructure in Azure to facilitate secure, Azure managed services for environments containing 25 or more managed or monitored service resources (devices).

- Provide an RMVA deployed within Client's Azure environment.
- Deploy and manage a single IPSec VPN tunnel which connects the Client's Azure environment to our Network Operations center (NOC). The IPSec VPN tunnel will be initiated from a Client dedicated firewall instance at Company and will terminate in Azure.
- Provide terminating infrastructure and connectivity services at Company Network Operations Center.
- Provide a dedicated security service instance (context) in Company NOC specifically for use with Azure and/or remote managed services utilizing highly available redundant hardware.
- Maintaining firewall operation including current and best supported service version.
- Defining and applying security best practices.
- Management of all service context configurations, including configuration updates and port openings/closures.
- Provide Client with a service specific list of port opening requirements to facilitate management services per technology under contract.
- Notify Client of IPSec VPN tunnel or RMVA connectivity issues.
- Monitor, maintain, and manage, RMVA.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of any service requirements, changes or modifications.
- Requires a subscription to Company s internet services.

Microsoft Azure Subscription

- Azure subscription and resources needed to support management of services in Azure
- Provide Azure monitoring resources Azure Monitor and Log Analytics for service monitoring
- Provide Company access to Azure Subscriptions and Resource Groups
- Azure subscription with available resources for:
  - A1 Basic instance for RMVA
  - VPN gateway
  - 1 private IP address

- Internet access for RMVA

600252 Remote Management Infrastructure for Azure (less than 25 devices)

Company's Responsibilities and Included Features

Secure connectivity from the Company Network Operations center (NOC) to the Client s Azure environment is required for Company to manage or monitor Client s Azure resources.

- Deploy and manage a single IPSec VPN tunnel which connects the Client's Azure environment to our Network Operations center (NOC). The IPSec VPN tunnel will be initiated from a Client dedicated firewall instance at Company and will terminate in Azure.
- Provide terminating infrastructure and connectivity services at Company Network Operations Center.
- Provide a dedicated security service instance (context) in Company NOC specifically for use with Azure and/or remote managed services utilizing highly available redundant hardware.
- Maintaining firewall operation including current and best supported service version.
- Defining and applying security best practices.
- Management of all service context configurations, including configuration updates and port openings/closures.
- Provide Client with a service specific list of port opening requirements to facilitate management services per technology under contract.
- Notify Client of IPSec VPN tunnel connectivity issues.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Notify Company of any service requirements, changes or modifications.
- Requires a subscription to Company s internet services.

Microsoft Azure Subscription

- Azure subscription and resources needed to support management of services in Azure
- Provide Azure monitoring resources Azure Monitor and Log Analytics for service monitoring
- Provide Company access to Azure Subscriptions and Resource Groups
- Azure subscription with available resources for:
  - VPN gateway

610418 Account Level Fixed - SD Executive

Company's Responsibilities and Included Features

Service Delivery Executive

- Provide a fully dedicated Service Delivery Executive to the Client.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Receive the service.

Category: Public Cloud

602537 Azure Cloud Support Services Basic

Company will provide reactive support for Azure incident and service requests during Company s normal business hours.

Service Parameters

- Incident and Requests - Service requests and incidents are limited to 2 service requests or incidents per month.
- Incident and Requests - Effort per incident/request is limited to 4 hours
- Changes in Azure limited to 4 hours per month

Definitions

- Incident An event triggered by an unplanned event or service interruption.
- Service Request - A request for support not triggered by an unplanned event or service interruption.
- Expert User - An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Company's Responsibilities and Included Features

Onboarding

- Company will provide the following onboarding activities at service inception:
    - Contacts and designated resources
    - Client specific documentation
    - Client training on how to request support
    - Assessment in scope items:
        - Privilege identity management policy
        - Health status
        - Roles
        - Administrative policy
        - Access policy
        - Policy settings
        - Notification settings
        - Identity governance review
        - Azure AD configuration and integration review.
        - Azure AD monitoring and alerting
    - Follow-up meeting with Client to review findings and discuss recommendations
    - OneNeck will provide the deliverables listed below in the identified format(s).
    - Findings summary: High level summary of areas that need improvement Excel document.
    - Detailed report: Detailed report with explanation of the recommendations Word document.
    - Azure standard settings
    - Azure Monitor Logs Workspace
    - Information technology service management (ITSM) set up
    - Assess Client s Azure current state issues and risks
    - Azure Identity Assessment - OneNeck engineer to perform high-level assessment of the Client s Azure Active Directory (AD) and Governance administrative configurations.
    - Mutually agreed upon subscription changes to enhance response and supportability

Service Requests

- Answer Azure questions and provide Azure guidance
- Provide relevant Microsoft documentation link
- Respond to service requests related to Azure incidents

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for Azure incident requests from Client, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Azure level troubleshooting

Escalation to Microsoft

- Document user issues and system errors

Azure Knowledge Base

- Access to curated Microsoft Azure documentation
- Access to OneNeck Azure Knowledge Articles

Service Delivery

- Service requests are to be requested through the Company Service Desk using portal, phone, or email.
- Support is limited to the number of incidents and service requests (collectively referred to as requests) per month as contracted. Based upon a rolling three (3) month average of requests consumed. Bursts in monthly consumption of requests may not exceed 200% of contracted monthly requests. Additional incidents and service requests can purchased under separate ItemID
- Annual Azure Support Assessment & Review
  - Discuss Azure support history
  - Service evaluation
  - Update contacts
- Company will provide support to the Client s Azure subscriptions, prioritized as follows:

Priority	Definition	Timescale	Incident Response Objective
1	One or more business critical application functions is impeding the customer s ability to perform business.	M-F, 7a-7p MST	2 Hours
2	One or more business critical application functions are degraded and is impacting the customer s ability to perform business.	M-F, 7a-7p MST	4 Hours
3	The incident has a medium impact on the customer's ability to perform business.	M-F, 7a-7p MST	12 Hours
4	The incident has a minor impact on the customer's ability to perform business.	M-F, 7a-7p MST	24 Hours
5	The incident has no impact to the customer s ability to perform business.	M-F, 7a-7p MST	36 Hours

- Azure support will be provided on a commercially reasonable basis for any time outside of the designated support hours, unless agreed upon in advance by both parties.

Expert User Technical Support*

- Technical support may only be requested by a Client Expert User*, available during the following hours
  - 7 am to 7 pm MST, Monday to Friday technical support for priority 1, 2, 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Application of Changes

- Application of solutions/steps to resolve incidents
- Limited to 4 hours per month
- Company will follow Customers change governance process

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Service Management

- Technical lead that can manage client side of Azure to provide
    - Company access to Azure tenants and subscriptions Resources
    - Resources
    - Change control and governance
    - Active participation in triage and troubleshooting
    - Coordination of validation testing
    - Must be capable to do these things:
        - Log into Azure portal
        - Make changes to resources In Azure
    - Identify named Client users authorized to make requests for Azure support
    - Support of non-Expert Users (typically refers to non-IT department staff or application end users)

Azure Subscriptions

- Client must obtain the Azure subscription(s) to be supported by Company through Company s Microsoft Cloud Service Provider program
- Service assumes existing Azure tenant and subscriptions in a stable state at onboarding. Company can provide remediation as a time and material project
- Any additional Azure resources consumed to enable troubleshooting and support such as Azure Monitor Logs and other troubleshooting resources

Workload Access and Administration

- Company will not have access to data, OS or other workloads unless contracted as a managed service
- Operating system support, administration, and management
- Database support, administration, and management
- Application support, administration, and management

Design, Deploy, Migration and Administration

- Perform setup, configuration, migration and administration of Azure Resources, integrations, data and applications, including but not limited to:
    - Virtual machines
    - Azure Active Directory
    - Active Directory
    - Azure AD connect integration
    - Network integrations and settings outside of Azure
- Runbook activities to maintain resources and applications
- Perform backup & restore operations
- Azure resource monitoring
- Azure alert monitoring
- Remediation of Azure environment from Audit findings or assessments
- Project work

Application and Script Development and Maintenance

- Application and script development, configuration, and support
- Application and content updates
- Third-party application dependencies

Security & Audit Requirements

- All security design, configuration, and operations
- Azure security alert incident response

- Azure resources for audit logging
- Backup retention requirements

Microsoft Standards and Notifications

- Monitoring of Microsoft notifications
- Perform Microsoft required changes to maintain current and standard configuration

Cost Management

- Reservation management
- Decisions on commitment

602538 Azure Cloud Support Service Standard

Company will provide reactive support for Azure incident and service requests during Company s normal business hours, as well as 24x7 business critical support.

Service Parameters

- Incident and Requests - Service requests and incidents are limited to 4 service requests or incidents per month.
- Incident and Requests - Effort per incident/request is limited to 4 hours
- Changes in Azure limited to 4 hours per month

Definitions

- Incident An event triggered by an unplanned event or service interruption.
- Service Request - A request for support not triggered by an unplanned event or service interruption.
- Expert User - An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Company's Responsibilities and Included Features

Onboarding

- Company will provide the following onboarding activities at service inception:
  - Information technology service management (ITSM) set up
    - Contacts and designated resources
    - Client specific documentation
    - Client training on how to request support
  - Assess Client s Azure current state issues and risks
  - Azure Identity Assessment - OneNeck engineer to perform high-level assessment of the Client s Azure Active Directory (AD) and Governance administrative configurations.
    - Assessment in scope items:
      - Identity governance review
        - Privilege identity management policy
      - Azure AD configuration and integration review.
        - Health status
        - Roles
        - Administrative policy
        - Access policy
      - Azure AD monitoring and alerting
        - Policy settings
        - Notification settings
    - Follow-up meeting with Client to review findings and discuss recommendations
    - OneNeck will provide the deliverables listed below in the identified format(s).
    - Findings summary: High level summary of areas that need improvement Excel document.

        - Detailed report: Detailed report with explanation of the recommendations Word document.
    - Mutually agreed upon subscription changes to enhance response and supportability
        - Azure standard settings
        - Azure Monitor Logs Workspace

Service Requests

- Answer Azure questions and provide Azure guidance
- Provide relevant Microsoft documentation link
- Respond to service requests related to Azure incidents

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for Azure incident requests from Client, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Azure level troubleshooting
    - Escalation to Microsoft
- Document user issues and system errors

Azure Knowledge Base

- Access to curated Microsoft Azure documentation
- Access to OneNeck Azure Knowledge Articles

Service Delivery

- Service requests are to be requested through the Company Service Desk using portal, phone, or email.
- Support is limited to the number of incidents and service requests (collectively referred to as requests) per month as contracted. Based upon a rolling three (3) month average of requests consumed. Bursts in monthly consumption of requests may not exceed 200% of contracted monthly requests. Additional incidents and service requests can purchased under separate ItemID
- Annual Azure Support Assessment & Review
    - Discuss Azure support history
    - Service evaluation
    - Update contacts
- Company will provide support to the Client s Azure subscriptions, prioritized as follows:

Priority	Definition	Timescale	Incident Response Objective
1	One or more business critical application functions is impeding the customer s ability to perform business.	24x7x365	2 Hours
2	One or more business critical application functions are degraded and is impacting the customer s ability to perform business.	24x7x365	4 Hours
3	The incident has a medium impact on the customer's ability to perform business.	M-F, 7a-7p MST	12 Hours
4	The incident has a minor impact on the customer's ability to perform business.	M-F, 7a-7p MST	24 Hours
5	The incident has no impact to the customer s ability to perform business.	M-F, 7a-7p MST	36 Hours

- Azure support will be provided on a commercially reasonable basis for any time outside of the designated support hours, unless agreed upon in advance by both parties.

Expert User Technical Support*

- Technical support may only be requested by a Client Expert User*, available during the following hours
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 7 am to 7 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Application of Changes

- Application of solutions/steps to resolve incidents
- Limited to 4 hours per month
- Company will follow Customers change governance process

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Service Management

- Technical lead that can manage client side of Azure to provide
  - Company access to Azure tenants and subscriptions Resources
  - Resources
  - Change control and governance
  - Active participation in triage and troubleshooting
  - Coordination of validation testing
  - Must be capable to do these things:
    - Log into Azure portal
    - Make changes to resources In Azure
  - Identify named Client users authorized to make requests for Azure support
  - Support of non-Expert Users (typically refers to non-IT department staff or application end users)

Azure Subscriptions

- Client must obtain the Azure subscription(s) to be supported by Company through Company s Microsoft Cloud Service Provider program
- Service assumes existing Azure tenant and subscriptions in a stable state at onboarding. Company can provide remediation as a time and material project
- Any additional Azure resources consumed to enable troubleshooting and support such as Azure Monitor Logs and other troubleshooting resources

Workload Access and Administration

- Company will not have access to data, OS or other workloads unless contracted as a managed service
- Operating system support, administration, and management
- Database support, administration, and management
- Application support, administration, and management

Design, Deploy, Migration and Administration

- Perform setup, configuration, migration and administration of Azure Resources, integrations, data and applications, including but not limited to:
  - Virtual machines
  - Azure Active Directory
  - Active Directory
  - Azure AD connect integration

        - Network integrations and settings outside of Azure
    - Runbook activities to maintain resources and applications
    - Perform backup & restore operations
    - Azure resource monitoring
    - Azure alert monitoring
    - Remediation of Azure environment from Audit findings or assessments
    - Project work

Application and Script Development and Maintenance

- Application and script development, configuration, and support
- Application and content updates
- Third-party application dependencies

Security & Audit Requirements

- All security design, configuration, and operations
- Azure security alert incident response
- Azure resources for audit logging
- Backup retention requirements

Microsoft Standards and Notifications

- Monitoring of Microsoft notifications
- Perform Microsoft required changes to maintain current and standard configuration

Cost Management

- Reservation management
- Decisions on commitment

602539 Azure Cloud Support Service Premium

Company will provide Azure guidance and recommendations for adoption and optimization of Azure subscriptions and resources. Company will provide reactive support for Azure incident and service requests during Company s normal business hours, as well as 24x7 business critical support.

Service Parameters

- Incident and Requests - Service requests and incidents are limited to 8 service requests or incidents per month.
- Incident and Requests - Effort per incident/request is limited to 4 hours
- Changes in Azure limited to 4 hours per month
- Cloud Adoption Follow up requests on Azure strategy is limited to 4 sessions per year
- Cost Optimization Cost optimization sessions are limited to 4 times per year

Definitions

- Incident An event triggered by an unplanned event or service interruption.
- Service Request - A request for support not triggered by an unplanned event or service interruption.
- Expert User - An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Company's Responsibilities and Included Features

Onboarding

- Company will provide the following onboarding activities at service inception:
    - Information technology service management (ITSM) set up

        - Contacts and designated resources
        - Client specific documentation
        - Client training on how to request support
    - Assess Client s Azure current state issues and risks
    - Azure Identity Assessment - OneNeck engineer to perform high-level assessment of the Client s Azure Active Directory (AD) and Governance administrative configurations.
        - Assessment in scope items:
            - Identity governance review
                - Privilege identity management policy
            - Azure AD configuration and integration review.
                - Health status
                - Roles
                - Administrative policy
                - Access policy
            - Azure AD monitoring and alerting
                - Policy settings
                - Notification settings
        - Follow-up meeting with Client to review findings and discuss recommendations
        - OneNeck will provide the deliverables listed below in the identified format(s).
        - Findings summary: High level summary of areas that need improvement Excel document.
        - Detailed report: Detailed report with explanation of the recommendations Word document.
    - Mutually agreed upon subscription changes to enhance response and supportability
        - Azure standard settings
        - Azure Monitor Logs Workspace

Adoption

Company will:

- Participate with client in annual strategy and planning meetings to provide guidance on utilizing Azure and advise on Microsoft standard practices
- Uilize Azure Advisor and Microsoft Azure Well-Architected Framework to make next step recommendations on reliability, security, cost and operational optimization, and performance efficiency
- Respond to follow up requests on Azure strategy and provide guidance up to 4 sessions per year
- Provide relevant Microsoft documentation links

Guided by Microsoft Azure Well-Architected Framework https://learn.microsoft.com/en-us/azure/well-architected/ and the Microsoft Cloud Adoption Framework for Azure https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/.

Cost Optimization

- Provide cost optimization awareness and recommendations using Azure Advisor up to 4 times per year
- Provide tailored recommendations, analysis and optimization plan, presented to the customer on an ongoing basis up to 4 times per year. (Some optimizations will require a project to implement, such as changing machine types, platform migrations, etc.)

Guided by Microsoft Azure Well-Architected Framework https://learn.microsoft.com/en-us/azure/well-architected/ and the Microsoft Cloud Adoption Framework for Azure https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/.

Service Requests

- Answer Azure questions and provide Azure guidance
- Provide relevant Microsoft documentation link
- Respond to service requests related to Azure incidents

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for Azure incident requests from Client, and research problems and

issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Azure level troubleshooting
    - Escalation to Microsoft
- Document user issues and system errors

Azure Knowledge Base

- Access to curated Microsoft Azure documentation
- Access to OneNeck Azure Knowledge Articles
- Client specific knowledge articles

Service Delivery

- Customer Success Manager/Service Delivery Manager designated Company key point of contact
- Service requests are to be requested through the Company Service Desk using portal, phone, or email.
- Support is limited to the number of incidents and service requests (collectively referred to as requests) per month as contracted. Based upon a rolling three (3) month average of requests consumed. Bursts in monthly consumption of requests may not exceed 200% of contracted monthly requests. Additional incidents and service requests can purchased under separate ItemID
- Annual Azure Support Assessment & Review
    - Discuss Azure support history
    - Service evaluation
    - Update contacts
- Company will provide support to the Client s Azure subscriptions, prioritized as follows:

Priority	Definition	Timescale	Incident Response Objective
1	One or more business critical application functions is impeding the customer s ability to perform business.	24x7x365	2 Hours
2	One or more business critical application functions are degraded and is impacting the customer s ability to perform business.	24x7x365	4 Hours
3	The incident has a medium impact on the customer's ability to perform business.	M-F, 7a-7p MST	12 Hours
4	The incident has a minor impact on the customer's ability to perform business.	M-F, 7a-7p MST	24 Hours
5	The incident has no impact to the customer s ability to perform business.	M-F, 7a-7p MST	36 Hours

- Azure support will be provided on a commercially reasonable basis for any time outside of the designated support hours, unless agreed upon in advance by both parties.

Expert User Technical Support*

- Technical support may only be requested by a Client Expert User*, available during the following hours
    - 24 x 7 technical support for priority 1 and 2 incidents
    - 7 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
    - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Application of Changes

- Application of solutions/steps to resolve incidents
- Limited to 4 hours per month
- Company will follow Customers change governance process

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Service Management

- Technical lead that can manage client side of Azure to provide
    - Company access to Azure tenants and subscriptions Resources
    - Resources
    - Change control and governance
    - Active participation in triage and troubleshooting
    - Coordination of validation testing
    - Must be capable to do these things:
        - Log into Azure portal
        - Make changes to resources In Azure
    - Identify named Client users authorized to make requests for Azure support
    - Support of non-Expert Users (typically refers to non-IT department staff or application end users)

Azure Subscriptions

- Client must obtain the Azure subscription(s) to be supported by Company through Company s Microsoft Cloud Service Provider program
- Service assumes existing Azure tenant and subscriptions in a stable state at onboarding. Company can provide remediation as a time and material project
- Any additional Azure resources consumed to enable troubleshooting and support such as Azure Monitor Logs and other troubleshooting resources

Workload Access and Administration

- Company will not have access to data, OS or other workloads unless contracted as a managed service
- Operating system support, administration, and management
- Database support, administration, and management
- Application support, administration, and management

Design, Deploy, Migration and Administration

- Perform setup, configuration, migration and administration of Azure Resources, integrations, data and applications, including but not limited to:
    - Virtual machines
    - Azure Active Directory
    - Active Directory
    - Azure AD connect integration
    - Network integrations and settings outside of Azure
- Runbook activities to maintain resources and applications
- Perform backup & restore operations
- Azure resource monitoring
- Azure alert monitoring
- Remediation of Azure environment from Audit findings or assessments
- Project work

Application and Script Development and Maintenance

- Application and script development, configuration, and support
- Application and content updates

- Third-party application dependencies

Security & Audit Requirements

- All security design, configuration, and operations
- Azure security alert incident response
- Azure resources for audit logging
- Backup retention requirements

Microsoft Standards and Notifications

- Monitoring of Microsoft notifications
- Perform Microsoft required changes to maintain current and standard configuration

Cost Management

- Reservation management
- Decisions on commitment

604380 Azure Reservation and Savings Plan Management

Company manages Azure reservations and savings plans and makes recommendations on new reservation and savings plan opportunities. Company modifies existing or adds new reservations and savings plans based on Client s approved changes.

Company's Responsibilities and Included Features

Service Setup

- Capture reservation and savings plan baseline
- Document ownership of each reservation and savings plan
- Document Client s reservation and savings plan strategy
- Review Azure Advisor Cost Optimization to understand targets and goals
- Establish a monthly review cycle with Client

Reservation and Savings Plan Review and Analysis

- Analyze Azure Advisor and existing reservation and savings plan status and utilization
- Make reservation and savings plan recommendations

Client Notification

- Submit recommendations to Client for approval

Reservation and Savings Plan Order and Changes

- Review approval request from Client
- Order or make changes to reservations and savings plans
- Update reservation and savings plan documentation
- Escalate issues to Client
- Resolve the approval request

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client is responsible for all contractual commitments made in Azure and adhering to Microsoft rules and policies pertaining to reservations and savings plans.

Identification of Resources and Owners

- Provide strategy and goal for reservations and savings plans
- Identify business owner for each reservation or savings plan

- Identify the tenants, subscriptions, resource groups and resources that will be the targets of reservations or savings plans

Access

- Provide Company access to Microsoft Online Services and Azure Resources

Client Business Owner

- Approve new reservations and savings plans or changes to reservations and savings plans
- Review recommendations
- Company assumes that the information provided during Client s meetings, ticket system and through documents is accurate and up-to-date. Incorrect information can result in risk over commitment, under-utilization, or reduced savings.
- Company assumes that the Client's business owners will be available in a timely manner for any discussion required for problem troubleshooting and resolution

Azure Subscriptions

- Client must obtain the Azure subscription(s) to be supported by Company through Company s Microsoft Cloud Service Provider program
- Service assumes existing Azure tenant and subscriptions in a stable state at onboarding. Company can provide remediation as a time and material project
- Any additional Azure resources consumed to enable troubleshooting and support such as Azure Monitor Logs and other troubleshooting resources

606651 Azure Load Balancer Administration

Company's Responsibilities and Included Features

Administration

- Managing and updating the Network Address Translation (NAT) and outbound rules as required
- Adding or removing servers from backend pools as needed
- Configuring and managing backend settings
- Updating load balancing rules as per changes in application endpoints
- Configuring and managing health probes to monitor the health of the backend servers
- Document applicable load balancer resource, administration procedures and policies
- Administration of backup of load balancer configuration to Azure storage repository

Security Administration

- Managing access permissions for the load balancer
- Azure Advisor Secure score review

Incident Triage and Troubleshooting

- Diagnosis of service incidents
- Triage of service incidents
- Troubleshoot and work to resolve service incidents
- Document service incidents
- Escalate incidents to Microsoft as needed

Monitoring

- Monitoring Load balancer performance and availability
- Setting up alerts for potential performance issues
- Availability and reliability monitoring

Performance monitoring
- Events monitoring

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes to be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client s staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Microsoft Azure Subscription

- Azure subscription and resources
- Provide Azure monitoring resources for Azure Monitor and Log Analytics for service monitoring
- Provide Company access to subscriptions

Security and Audit

- Encryption
- Provide audit requirements
- Provide Azure resources for audit logging

Application and Dependencies

- Optimizing the load balancer for cost
- Application and content updates
- Third-party application dependencies

Deployment

- Creation and deployment of new load balancers and instances
- Repurpose or migration of load balancers

End User Support

- Support of non-Expert Users (typically refers to non-IT department staff or application end users)

611269 Azure Network Resource Support for Flowserve

Company will support the administration of Azure network resources deployed in a Microsoft Azure environment.

Definitions

- Incident An event triggered by an unplanned event or service interruption.
- Service Request - A request for support not triggered by an unplanned event or service interruption.
- Change - A change is any addition, modification, or removal of an Azure resource.

Company's Responsibilities and Included Features

Support

Administration of Azure network resources listed below
    - Virtual Network (VNET)
    - Network Security Groups (NSG)
    - Load Balancer
    - Application Gateway
    - VPN Gateway
- Optimization of the Azure network resources based on Client s approved requests
- Changes to the existing Azure in-scope network resources
- Major changes are outside of the scope of this ItemID and may be provided on a separately contracted time and materials project basis

Recommendations and Review

- Advise Client on the Azure network resources configuration
- Review of the Azure network resources objects

Service Requests

- Answer Azure questions and provide Azure guidance
- Provide relevant Microsoft documentation link
- Respond to service requests related to Azure incidents

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for Azure incident requests from Client, and research problems and issues, utilizing:
    - Company knowledge of known errors and their potential solutions
    - General Azure level troubleshooting
    - Escalation to Microsoft
- Document user issues and system errors

Terms

- Notwithstanding the term of this Statement of Work, this Offering is provided on a month-to-month basis.
- Company may revise the terms of use or pricing with 30 days notice.

Azure Knowledge Base

- Access to curated Microsoft Azure documentation
- Access to OneNeck Azure Knowledge Articles
- Client specific knowledge articles

Service Delivery

- Customer Success Manager/Service Delivery Manager designated Company key point of contact
- Service requests are to be requested through the Company Service Desk using portal, phone, or email.
- Company will provide support to the Client s Azure subscriptions, prioritized as follows:

Priority	Definition	Timescale	Incident Response Objective
1	One or more business critical application functions is impeding the customer s ability to perform business.	24x7x365	2 Hours
2	One or more business critical application functions are degraded and is impacting the customer s ability to perform business.	24x7x365	4 Hours
	The incident has a medium impact on the customer's ability to perform	M-F, 7am-7pm	

3	business.	MST	12 Hours
4	The incident has a minor impact on the customer's ability to perform business.	M-F, 7am-7pm MST	24 Hours
5	The incident has no impact to the customer s ability to perform business.	M-F, 7am-7pm MST	36 Hours

- Azure support will be provided on a commercially reasonable basis for any time outside of the designated support hours, unless agreed upon in advance by both parties.

Expert User Technical Support*

- Technical support may only be requested by a Client Expert User*, available during the following hours
  - 24 x 7 technical support for priorities 1 and 2 incidents
  - 7 am to 5 pm MST, Monday to Friday technical support for priorities 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client's staff, whichever is greater.

Application of Changes

- Application of solutions/steps to resolve incidents
- Company will follow Customers change governance process

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Service Management

- Technical lead that can manage client's side of Azure to provide
  - Company access to Azure tenants and subscriptions Resources
  - Resources
  - Change control and governance
  - Active participation in triage and troubleshooting
  - Coordination of validation testing
  - Must be capable to do these things:
    - Log into Azure portal
    - Make changes to resources In Azure
  - Identify named Client's named users authorized to make requests for Azure support
  - Support of non-Expert Users (typically refers to non-IT department staff or application end users)

Azure Subscriptions

- Client must obtain the Azure subscription(s) to be supported by Company through Company s Microsoft Cloud Service Provider program
- Service assumes that existing Azure tenant and subscriptions are in a stable state at onboarding. Company can provide remediation as a time and material project
- Any additional Azure resources consumed to enable troubleshooting and support, such as Azure Monitor Logs and other troubleshooting resources

Workload Access and Administration

- Company will not have access to data, OS or other workloads unless contracted as a managed service
- Operating system support, administration, and management
- Database support, administration, and management

- Application support, administration, and management

Design, Deploy, Migration and Administration

- Perform setup, configuration, migration and administration of Azure Resources, integrations, data and applications, including but not limited to:
  - Virtual machines
  - Azure Active Directory
  - Active Directory
  - Azure AD connect integration
  - Network integrations and settings outside of Azure
- Runbook activities to maintain resources and applications
- Perform backup & restore operations
- Azure resource monitoring
- Azure alert monitoring
- Remediation of Azure environment from Audit findings or assessments
- Project work

Application and Script Development and Maintenance

- Application and script development, configuration, and support
- Application and content updates
- Third-party application dependencies

Security & Audit Requirements

- All security design, configuration, and operations
- Azure security alert incident response
- Azure resources for audit logging
- Backup retention requirements

Microsoft Standards and Notifications

- Monitoring of Microsoft notifications
- Perform Microsoft required changes to maintain current and standard configuration

Cost Management

- Reservation management
- Decisions on commitment

611658 Azure Cloud Support Service Premium Enterprise

Company will provide Azure guidance and recommendations for adoption and optimization of Azure subscriptions and resources. Company will provide reactive support for Azure incident and service requests during Company's normal business hours, as well as 24x7 business critical support.

Service Parameters

- Incident and Requests - Service requests and incidents are limited to 8 service requests or incidents per month.
- Incident and Requests - Effort per incident/request is limited to 4 hours
- Changes in Azure limited to 4 hours per month
- Cloud Adoption – Follow up requests on Azure strategy is limited to 4 sessions per year
- Cost Optimization – Cost optimization sessions are limited to 4 times per year

Definitions

- Incident – An event triggered by an unplanned event or service interruption.

Service Request - A request for support not triggered by an unplanned event or service interruption.

- Expert User - An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Company's Responsibilities and Included Features

Onboarding

- Company will provide the following onboarding activities at service inception:
    - Information technology service management (ITSM) set up
        - Contacts and designated resources
        - Client specific documentation
        - Client training on how to request support
    - Assess Client's Azure current state issues and risks
    - Azure Identity Assessment - OneNeck engineer to perform high-level assessment of the Client's Azure Active Directory (AD) and Governance administrative configurations.
        - Assessment in scope items:
            - Identity governance review
                - Privilege identity management policy
            - Azure AD configuration and integration review.
                - Health status
                - Roles
                - Administrative policy
                - Access policy
            - Azure AD monitoring and alerting
                - Policy settings
                - Notification settings
        - Follow-up meeting with Client to review findings and discuss recommendations
        - OneNeck will provide the deliverables listed below in the identified format(s).
        - Findings summary: High level summary of areas that need improvement – Excel document.
        - Detailed report: Detailed report with explanation of the recommendations – Word document.
    - Mutually agreed upon subscription changes to enhance response and supportability
        - Azure standard settings
        - Azure Monitor Logs Workspace

Adoption

Company will:

- Participate with client in annual strategy and planning meetings to provide guidance on utilizing Azure and advise on Microsoft standard practices
- Uilize Azure Advisor and Microsoft Azure Well-Architected Framework to make next step recommendations on reliability, security, cost and operational optimization, and performance efficiency
- Respond to follow up requests on Azure strategy and provide guidance up to 4 sessions per year
- Provide relevant Microsoft documentation links

Guided by Microsoft Azure Well-Architected Framework https://learn.microsoft.com/en-us/azure/well-architected/ and the Microsoft Cloud Adoption Framework for Azure https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/.

Cost Optimization

- Provide cost optimization awareness and recommendations using Azure Advisor up to 4 times per year
- Provide tailored recommendations, analysis and optimization plan, presented to the customer on an ongoing basis up to 4 times per year. (Some optimizations will require a project to implement, such as changing machine types, platform migrations, etc.)

Guided by Microsoft Azure Well-Architected Framework https://learn.microsoft.com/en-us/azure/well-architected/ and the Microsoft Cloud Adoption Framework for Azure https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/.

Service Requests

- Answer Azure questions and provide Azure guidance
- Provide relevant Microsoft documentation link
- Respond to service requests related to Azure incidents

Incident Triage and Troubleshooting

- Triage and manage the troubleshooting process for Azure incident requests from Client, and research problems and issues, utilizing:
  - Company knowledge of known errors and their potential solutions
  - General Azure level troubleshooting
  - Escalation to Microsoft
- Document user issues and system errors

Azure Knowledge Base

- Access to curated Microsoft Azure documentation
- Access to OneNeck Azure Knowledge Articles
- Client specific knowledge articles

Service Delivery

- Customer Success Manager/Service Delivery Manager – designated Company key point of contact
- Service requests are to be requested through the Company Service Desk using portal, phone, or email.
- Support is limited to the number of incidents and service requests (collectively referred to as requests) per month as contracted. Based upon a rolling three (3) month average of requests consumed. Bursts in monthly consumption of requests may not exceed 200% of contracted monthly requests. Additional incidents and service requests can purchased under separate ItemID
- Annual Azure Support Assessment & Review
  - Discuss Azure support history
  - Service evaluation
  - Update contacts
- Company will provide support to the Client's Azure subscriptions, prioritized as follows:

Priority	Definition	Timescale	Incident Response Objective
1	One or more business critical application functions is impeding the customer's ability to perform business.	24x7x365	2 Hours
2	One or more business critical application functions are degraded and is impacting the customer's ability to perform business.	24x7x365	4 Hours
3	The incident has a medium impact on the customer's ability to perform business.	M-F, 7a-7p MST	12 Hours
4	The incident has a minor impact on the customer's ability to perform business.	M-F, 7a-7p MST	24 Hours
5	The incident has no impact to the customer's ability to perform business.	M-F, 7a-7p MST	36 Hours

- Azure support will be provided on a commercially reasonable basis for any time outside of the designated support hours, unless agreed upon in advance by both parties.

Expert User Technical Support*

- Technical support may only be requested by a Client Expert User*, available during the following hours
  - 24 x 7 technical support for priority 1 and 2 incidents
  - 7 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
  - Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Application of Changes

- Application of solutions/steps to resolve incidents
- Limited to 4 hours per month
- Company will follow Customers change governance process

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Service Management

- Technical lead that can manage client side of Azure to provide
  - Company access to Azure tenants and subscriptions Resources
  - Resources
  - Change control and governance
  - Active participation in triage and troubleshooting
  - Coordination of validation testing
  - Must be capable to do these things:
    - Log into Azure portal
    - Make changes to resources In Azure
  - Identify named Client users authorized to make requests for Azure support
  - Support of non-Expert Users (typically refers to non-IT department staff or application end users)

Azure Subscriptions

- Client must enable access to the Azure subscription(s) to be supported by Company
- Service assumes existing Azure tenant and subscriptions in a stable state at onboarding. Company can provide remediation as a time and material project
- Any additional Azure resources consumed to enable troubleshooting and support such as Azure Monitor Logs and other troubleshooting resources

Workload Access and Administration

- Company will not have access to data, OS or other workloads unless contracted as a managed service
- Operating system support, administration, and management
- Database support, administration, and management
- Application support, administration, and management

Design, Deploy, Migration and Administration

- Perform setup, configuration, migration and administration of Azure Resources, integrations, data and applications, including but not limited to:
  - Virtual machines
  - Azure Active Directory
  - Active Directory
  - Azure AD connect integration
  - Network integrations and settings outside of Azure

- Runbook activities to maintain resources and applications
- Perform backup & restore operations
- Azure resource monitoring
- Azure alert monitoring
- Remediation of Azure environment from Audit findings or assessments
- Project work

Application and Script Development and Maintenance

- Application and script development, configuration, and support
- Application and content updates
- Third-party application dependencies

Security & Audit Requirements

- All security design, configuration, and operations
- Azure security alert incident response
- Azure resources for audit logging
- Backup retention requirements

Microsoft Standards and Notifications

- Monitoring of Microsoft notifications
- Perform Microsoft required changes to maintain current and standard configuration

Cost Management

- Reservation management
- Decisions on commitment

Family: Microsoft Azure

Category: Azure

606855 Azure Provisioned Throughput Units (PTU s) Prepay

Prepayment for Azure Usage

Company's Responsibilities and Included Features

- None

Prepayment for Azure Usage

Company's Responsibilities and Included Features

- None

Family: Third Party Services

Category: Accessories

600385 Toll-Free Number Implementation

Company's Responsibilities and Included Features

- Facilitate implementation of additional toll-free number to existing service.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- None

600466 Business Continuity - Automatic Reroute Feature Add

Company's Responsibilities and Included Features

Add the Business Continuity - Automatic Reroute feature to an existing toll-free number environment with the following attributes:

- Type = Basic
- Configuration = Trunk group call forward to a single telephone number
- Number Call Paths = 6

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Existing toll-free PRI service

600467 Setup - Business Continuity - Automatic Reroute Feature Add

Company's Responsibilities and Included Features

Setup the Business Continuity - Automatic Reroute feature to an existing toll-free number environment with the following attributes:

- Type = Basic
- Configuration = Trunk group call forward to a single telephone number
- Number Call Paths = 6

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Existing toll-free PRI service

606859 Microsoft Software License Review by Miro Consulting

Company's Responsibilities and Included Features

This ItemID 606859 contains an order for Professional Services provided by Miro Consulting, Inc. Client agrees, acknowledges, and understands that the actual performance of the Miro Consulting offerings will be provided by Miro Consulting, Inc. and may be subject to change as determined by Miro Consulting, Inc.

Microsoft Software License Review By Miro Consulting, Inc.

- License Position Assessment
- License Optimization
- Negotiation Support

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Terms

- Client agrees, acknowledges, and understands that the actual performance of the Miro Consulting offerings will be provided by Miro Consulting, Inc. and may be subject to change as determined by Miro Consulting, Inc.

- Miro Consulting, Inc. has granted OneNeck the right to sell a license to end users to use such offerings, on the condition that each such end user unconditionally agrees that the license will be governed by, and the parties will be subject to, the terms of the Miro Consulting, Inc. Terms of Service.
- In acknowledgement of the foregoing and intending to be bound thereby, Client agrees that Miro Consulting, Inc. offerings provided herein are subject to the Miro Consulting, Inc. Terms of Service, which are hereby incorporated into this Executed Order as Exhibit A.
- Client agrees that in its acknowledgement and acceptance of the Miro Consulting, Inc. Terms of Service, Client is solely responsible for its own compliance with the Miro Consulting, Inc. Terms of Service and does not assume any liability for OneNeck s acts, omissions or breaches of the Miro Consulting, Inc. Terms of Service.

Category: Alert Logic MSP

601879 Alert Logic MDR Professional M

Management of the Alert Logic MDR solution will only be applicable under the condition that Client has agreed for Company to also manage their firewalls and mission critical operating systems. Company will provide managed services in support of the Alert Logic, Inc. services and/or products specified herein, per Professional node purchased.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Professional

Alert Logic MDR Professional is an Alert Logic Hosted Service. Designed to protect environments classified as moderate or high risk, Alert Logic MDR Professional provides fully outsourced 24/7 threat detection for traditional, hybrid, and cloud infrastructures and applications accompanied by actionable guidance to enable customers to quickly respond to attacks.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection
- Network packet monitoring
- Log data monitoring

Company's Responsibilities and Included Features

Support Services

- Monitor security events. Incidents noted on non-Company-managed Operating Systems (OS) will be escalated to Client
- Update deployment assets and scope of coverage based on changes to protected environment
- Manage monitored network configuration for protected environment scope
- Manage network changes (span port changes, vlan changes, VPC changes, etc.) in Client s production environment
- Monitor Alert Logic agent

Support Services on Company-Managed Operating Systems (OS)

The following services are included on Company-managed OSs only as requested and/or approved by Client:

- Manage configuration and vulnerability remediation activities
- Manage security events and escalation

Reporting

- Provide security incident digest reports
- Provide and review Alert Logic value reports with Client at least once per quarter
- Review current usage against the solution and license parameters
- Review monthly Alert Logic health report with Client to discuss the remediation of coverage gaps

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Professional
- Alert Logic Remote Log Collector, available under separate ItemID, must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

Log usage for MDR Professional nodes may not exceed an aggregated average of 100 MB/Day/Node in any calendar quarter. Client agrees to pay any and all additional fees that Alert Logic charges for any log usage overages by Client.

A detailed service description of Alert Logic MDR Professional will be provided to Client upon request.

601949 Alert Logic MDR Professional M- Max Nodes 250

Company will provide managed services in support of the Alert Logic, Inc. services and/or products specified herein, for a maximum of 250 Professional nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Professional

Alert Logic MDR Professional is an Alert Logic Hosted Service. Designed to protect environments classified as moderate or high risk, Alert Logic MDR Professional provides fully outsourced 24/7 threat detection for traditional, hybrid, and cloud infrastructures and applications accompanied by actionable guidance to enable customers to quickly respond to attacks.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection
- Network packet monitoring
- Log data monitoring

Company's Responsibilities and Included Features

Support Services

- Monitor security events. Incidents noted on non-Company-managed Operating Systems (OS) will be escalated to Client
- Update deployment assets and scope of coverage based on changes to protected environment
- Manage monitored network configuration for protected environment scope
- Manage network changes (span port changes, vlan changes, VPC changes, etc.) in Client s production environment
- Monitor Alert Logic agent

Support Services on Company-Managed Operating Systems (OS)

The following services are included on Company-managed OSs only as requested and/or approved by Client:

- Manage configuration and vulnerability remediation activities
- Manage security events and escalation

Reporting

- Provide security incident digest reports
- Provide and review Alert Logic value reports with Client at least once per quarter
- Review current usage against the solution and license parameters
- Review monthly Alert Logic health report with Client to discuss the remediation of coverage gaps

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Professional
- Alert Logic Remote Log Collector, available under separate ItemID, must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable),

configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

Log usage for MDR Professional nodes may not exceed an aggregated average of 100 MB/Day/Node in any calendar quarter. Client agrees to pay any and all additional fees that Alert Logic charges for any log usage overages by Client.

A detailed service description of Alert Logic MDR Professional will be provided to Client upon request.

601950 Alert Logic MDR Professional M - Max Nodes 500

Company will provide managed services in support of the Alert Logic, Inc. services and/or products specified herein, for a maximum of 500 Professional nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Professional

Alert Logic MDR Professional is an Alert Logic Hosted Service. Designed to protect environments classified as moderate or high risk, Alert Logic MDR Professional provides fully outsourced 24/7 threat detection for traditional, hybrid, and cloud infrastructures and applications accompanied by actionable guidance to enable customers to quickly respond to attacks.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection
- Network packet monitoring
- Log data monitoring

Company's Responsibilities and Included Features

Support Services

- Monitor security events. Incidents noted on non-Company-managed Operating Systems (OS) will be escalated to Client
- Update deployment assets and scope of coverage based on changes to protected environment
- Manage monitored network configuration for protected environment scope
- Manage network changes (span port changes, vlan changes, VPC changes, etc.) in Client s production environment
- Monitor Alert Logic agent

Support Services on Company-Managed Operating Systems (OS)

The following services are included on Company-managed OSs only as requested and/or approved by Client:

- Manage configuration and vulnerability remediation activities
- Manage security events and escalation

Reporting

- Provide security incident digest reports
- Provide and review Alert Logic value reports with Client at least once per quarter

- Review current usage against the solution and license parameters
- Review monthly Alert Logic health report with Client to discuss the remediation of coverage gaps

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Professional
- Alert Logic Remote Log Collector, available under separate ItemID, must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

Log usage for MDR Professional nodes may not exceed an aggregated average of 100 MB/Day/Node in any calendar quarter. Client agrees to pay any and all additional fees that Alert Logic charges for any log usage overages by Client.

A detailed service description of Alert Logic MDR Professional will be provided to Client upon request.

601951 Alert Logic MDR Professional M - Max Nodes 750

Company will provide managed services in support of the Alert Logic, Inc. services and/or products specified herein, for a maximum of 750 Professional nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Professional

Alert Logic MDR Professional is an Alert Logic Hosted Service. Designed to protect environments classified as moderate or high risk, Alert Logic MDR Professional provides fully outsourced 24/7 threat detection for traditional, hybrid, and cloud infrastructures and applications accompanied by actionable guidance to enable customers to quickly respond to attacks.

Key Features include:

- Asset discovery

- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection
- Network packet monitoring
- Log data monitoring

Company's Responsibilities and Included Features

Support Services

- Monitor security events. Incidents noted on non-Company-managed Operating Systems (OS) will be escalated to Client
- Update deployment assets and scope of coverage based on changes to protected environment
- Manage monitored network configuration for protected environment scope
- Manage network changes (span port changes, vlan changes, VPC changes, etc.) in Client s production environment
- Monitor Alert Logic agent

Support Services on Company-Managed Operating Systems (OS)

The following services are included on Company-managed OSs only as requested and/or approved by Client:

- Manage configuration and vulnerability remediation activities
- Manage security events and escalation

Reporting

- Provide security incident digest reports
- Provide and review Alert Logic value reports with Client at least once per quarter
- Review current usage against the solution and license parameters
- Review monthly Alert Logic health report with Client to discuss the remediation of coverage gaps

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Professional
- Alert Logic Remote Log Collector, available under separate ItemID, must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues

- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

Log usage for MDR Professional nodes may not exceed an aggregated average of 100 MB/Day/Node in any calendar quarter. Client agrees to pay any and all additional fees that Alert Logic charges for any log usage overages by Client.

A detailed service description of Alert Logic MDR Professional will be provided to Client upon request.

601952 Alert Logic MDR Professional M- Max Nodes 1000

Company will provide managed services in support of the Alert Logic, Inc. services and/or products specified herein, for a maximum of 1,000 Professional nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Professional

Alert Logic MDR Professional is an Alert Logic Hosted Service. Designed to protect environments classified as moderate or high risk, Alert Logic MDR Professional provides fully outsourced 24/7 threat detection for traditional, hybrid, and cloud infrastructures and applications accompanied by actionable guidance to enable customers to quickly respond to attacks.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection
- Network packet monitoring
- Log data monitoring

Company's Responsibilities and Included Features

Support Services

- Monitor security events. Incidents noted on non-Company-managed Operating Systems (OS) will be escalated to Client
- Update deployment assets and scope of coverage based on changes to protected environment
- Manage monitored network configuration for protected environment scope
- Manage network changes (span port changes, vlan changes, VPC changes, etc.) in Client s production environment
- Monitor Alert Logic agent

Support Services on Company-Managed Operating Systems (OS)

The following services are included on Company-managed OSs only as requested and/or approved by Client:

- Manage configuration and vulnerability remediation activities
- Manage security events and escalation

Reporting

- Provide security incident digest reports
- Provide and review Alert Logic value reports with Client at least once per quarter
- Review current usage against the solution and license parameters
- Review monthly Alert Logic health report with Client to discuss the remediation of coverage gaps

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Professional
- Alert Logic Remote Log Collector, available under separate ItemID, must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

Log usage for MDR Professional nodes may not exceed an aggregated average of 100 MB/Day/Node in any calendar quarter. Client agrees to pay any and all additional fees that Alert Logic charges for any log usage overages by Client.

A detailed service description of Alert Logic MDR Professional will be provided to Client upon request.

601953 Alert Logic MDR Professional M - Max Nodes >1000

Company will provide managed services in support of the Alert Logic, Inc. services and/or products specified herein, per Professional node purchased over 1,000 Professional nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Professional

Alert Logic MDR Professional is an Alert Logic Hosted Service. Designed to protect environments classified as moderate or high risk, Alert Logic MDR Professional provides fully outsourced 24/7 threat detection for traditional, hybrid, and cloud infrastructures and applications accompanied by actionable guidance to enable customers to quickly respond to attacks.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks

Endpoint detection
- Network packet monitoring
- Log data monitoring

Company's Responsibilities and Included Features

Support Services

- Monitor security events. Incidents noted on non-Company-managed Operating Systems (OS) will be escalated to Client
- Update deployment assets and scope of coverage based on changes to protected environment
- Manage monitored network configuration for protected environment scope
- Manage network changes (span port changes, vlan changes, VPC changes, etc.) in Client s production environment
- Monitor Alert Logic agent

Support Services on Company-Managed Operating Systems (OS)

The following services are included on Company-managed OSs only as requested and/or approved by Client:

- Manage configuration and vulnerability remediation activities
- Manage security events and escalation

Reporting

- Provide security incident digest reports
- Provide and review Alert Logic value reports with Client at least once per quarter
- Review current usage against the solution and license parameters
- Review monthly Alert Logic health report with Client to discuss the remediation of coverage gaps

Expert User Technical Support*

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook.

* An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Professional
- Alert Logic Remote Log Collector, available under separate ItemID, must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for

monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

Log usage for MDR Professional nodes may not exceed an aggregated average of 100 MB/Day/Node in any calendar quarter. Client agrees to pay any and all additional fees that Alert Logic charges for any log usage overages by Client.

A detailed service description of Alert Logic MDR Professional will be provided to Client upon request.

601962 Alert Logic MDR Enterprise M

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Enterprise

Alert Logic MDR Enterprise is an Alert Logic Hosted Service that augments the Alert Logic MDR Professional Service. An Alert Logic security analyst is assigned to the Client who will develop knowledge of the Client s security environment to enable recommendations for continual advancement in Client s security posture.

Key Features include:

- Continuous threat hunting
- Proactive tuning and sensor optimization
- Extended security investigations
- Weekly security review
- Annual on-site

Minimum Requirements

Client must purchase and maintain an Alert Logic MDR Professional service to add the Alert Logic MDR Enterprise service.

A detailed service description of Alert Logic MDR Enterprise will be provided to Client upon request.

601963 Alert Logic Managed WAF M 1-5 Websites

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic Managed WAF

Alert Logic Managed WAF (Web Application Firewall) is an Alert Logic Hosted Service that provides inline web application protection by detecting and blocking potential threats from reaching Client web applications. The Alert Logic Managed WAF service includes ActiveWatch. Alert Logic ActiveWatch leverages Alert Logic ActiveIntelligence, ActiveAnalytics, Data Science Experts, Web Application Security Experts and the Security Analysts in Alert Logic s Security Operations Centers to provide application policy configuration, tuning and guidance.

Minimum Appliance Requirements

- An Alert Logic WAF Appliance must be deployed on assets that Client wants to protect with Alert Logic Managed WAF
- WAF Appliances may be physical or virtual depending upon deployment and service elections
- WAF Appliances must be deployed in pairs; high availability/redundancy is required to ensure service consistency

A detailed service description of Alert Logic Managed WAF will be provided to Client upon request.

601966 Alert Logic Managed WAF M 6-10 Websites

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert

Logic Addendum.

Alert Logic Managed WAF

Alert Logic Managed WAF (Web Application Firewall) is an Alert Logic Hosted Service that provides inline web application protection by detecting and blocking potential threats from reaching Client web applications. The Alert Logic Managed WAF service includes ActiveWatch. Alert Logic ActiveWatch leverages Alert Logic ActiveIntelligence, ActiveAnalytics, Data Science Experts, Web Application Security Experts and the Security Analysts in Alert Logic s Security Operations Centers to provide application policy configuration, tuning and guidance.

Minimum Appliance Requirements

- An Alert Logic WAF Appliance must be deployed on assets that Client wants to protect with Alert Logic Managed WAF
- WAF Appliances may be physical or virtual depending upon deployment and service elections
- WAF Appliances must be deployed in pairs; high availability/redundancy is required to ensure service consistency

A detailed service description of Alert Logic Managed WAF will be provided to Client upon request.

601967 Alert Logic Managed WAF M Additional Websites

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic Managed WAF

Alert Logic Managed WAF (Web Application Firewall) is an Alert Logic Hosted Service that provides inline web application protection by detecting and blocking potential threats from reaching Client web applications. The Alert Logic Managed WAF service includes ActiveWatch. Alert Logic ActiveWatch leverages Alert Logic ActiveIntelligence, ActiveAnalytics, Data Science Experts, Web Application Security Experts and the Security Analysts in Alert Logic s Security Operations Centers to provide application policy configuration, tuning and guidance.

Minimum Appliance Requirements

- An Alert Logic WAF Appliance must be deployed on assets that Client wants to protect with Alert Logic Managed WAF
- WAF Appliances may be physical or virtual depending upon deployment and service elections
- WAF Appliances must be deployed in pairs; high availability/redundancy is required to ensure service consistency

A detailed service description of Alert Logic Managed WAF will be provided to Client upon request.

602065 Alert Logic IDS Appliance M - Virtual

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic Intrusion Detection System (IDS) Appliances

An Alert Logic IDS Appliance must be deployed on assets that Client wants to protect with Alert Logic MDR Professional or Alert Logic MDR Essentials. At least one Alert Logic IDS Appliance is required for each environment protected. Alert Logic will provide all appliances.

System Requirements for Virtual IDS Appliances

Virtual CPU Cores	**Components**	**System Requirements**
4 cores	RAM	16 GB
4 cores	Disk space	40 GB Minimum
4 cores	Supported virtual environment	VMware, Hyper-V, AHV
		TLS Standard (SSL): 2048-bit key

4 cores	Encryption	encryption, 256-bit AES bulk encryption
4 cores	Peak supported throughput	500 Mbps
8 cores	RAM	32 GB
8 cores	Disk space	40 GB Minimum
8 cores	Supported virtual environment	VMware, Hyper-V, AHV
8 cores	Encryption	TLS Standard (SSL): 2048-bit key encryption, 256-bit AES bulk encryption
8 cores	Peak supported throughput	1 Gbps
16 cores	RAM	64 GB
16 cores	Disk space	40 GB Minimum
16 cores	Supported virtual environment	VMware, Hyper-V, AHV
16 cores	Encryption	TLS Standard (SSL): 2048-bit key encryption, 256-bit AES bulk encryption
16 cores	Peak supported throughput	2 Gbps (1 Gbps per fiber interface)

Company's Responsibilities and Included Features

Support Services

Monitor Alert Logic IDS appliance health.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Client must provide virtual service resources sufficient to meet the minimum Alert Logic Virtual Appliance requirements defined at https://docs.alertlogic.com/requirements/appliance-requirements.htm
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum

602066 Alert Logic WAF Appliance M - Virtual

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic WAF Appliances

An Alert Logic WAF Appliance must be deployed on assets that Client wants to protect with Alert Logic Managed WAF. WAF Appliances may be physical or virtual depending upon deployment and service elections. WAF Appliances must be deployed in pairs; high availability/redundancy is required to ensure service consistency. Alert Logic will provide all appliances.

System Requirements for Virtual WAF Appliances

Components	**System Requirements**
CPU	2 CPUs 64 bit
RAM	4 GB
Disk space	250 GB
Virtual network interface(s)	An interface with an external IP address for management; an interface with access to the web servers to be protected

Encryption/Decryption for SSL traffic	AES-NI CPU instruction set for encryption/decryption of SSL traffic on VMs and host OS is recommended
Clustering	For clustering to work, ensure promiscuous mode, forged transmits, and MAC address changes are allowed on the VMware virtual switch (vSwitch) or the port group in the VMware ESX network configuration

602067 Alert Logic Log Collector M - Windows

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic Remote Log Collector

With Alert Logic MDR Professional Services, an Alert Logic remote log collector must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic. The Alert Logic syslog remote collector agent software is installed on a VMware Windows server dedicated to the collection of syslog data.

Company's Responsibilities and Included Features

Support Services

- Maintain Alert Logic remote log collector server including:
  - Operating system (OS) patching
  - OS monitoring
- Monitor log sources to verify data is flowing to remote log collector

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

Operating System Software Licensing

- Procure OS software and licensing for current version of OS, including any user access licensing
- Procure current software maintenance where applicable

Antivirus Protection Software Licensing and Management

- Procurement of antivirus protection software, licensing and maintenance for current version of OS
- Installation of antivirus software
- Management of antivirus software and updates

Virtualization Platform

- Provide server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide Company with console access to the OS

Backup Job Administration and Backup Infrastructure

Backup Job Administration

- Administration of server backup jobs
- Installation and maintenance of agents
- Performance of backup restores

Backup System

- Provide backup system to enable backup of data from the server being used to contain the remote log collector via:
  - Contracted usage of a Company backup service which includes server backup job management

  OR

  - Procurement of backup server and agent licensing with available disk storage
  - Administration of backup system
  - Provide tape media and tape storage (if applicable)

Fulfill Client responsibilities outlined within the attached Alert Logic Addendum

602068 Alert Logic Log Collector M - Linux

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic Remote Log Collector

With Alert Logic MDR Professional Services, an Alert Logic remote log collector must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic. The Alert Logic syslog remote collector agent software is installed on a VMware Linux server dedicated to the collection of syslog data.

Company's Responsibilities and Included Features

Support Services

- Maintain Alert Logic remote log collector server including:
  - Operating system (OS) patching
  - OS monitoring
- Monitor log sources to verify data is flowing to remote log collector

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

Operating System Software Licensing

- Procure OS software and licensing for current version of OS, including any user access licensing
- Procure current software maintenance where applicable
- End-user access licensing
- Application and database licensing, if applicable

Antivirus Protection Software Licensing and Management

- Procurement of antivirus protection software, licensing and maintenance for current version of OS
- Installation of antivirus software
- Management of antivirus software and updates

Virtualization Platform

- Provide server host hardware (Disk, CPU and RAM)
- Provide licensed virtualization software
- Manage virtualization platform
- Provide Company with console access to the OS

Backup Job Administration and Backup Infrastructure

Backup Job Administration

- Administration of server backup jobs
- Installation and maintenance of agents
- Performance of backup restores

Backup System

- Provide backup system to enable backup of data from the server being used to contain the remote log collector via:
  - Contracted usage of a Company backup service which includes server backup job management

  OR

  - Procurement of backup server and agent licensing with available disk storage
  - Administration of backup system
  - Provide tape media and tape storage (if applicable)

Fulfill Client responsibilities outlined within the attached Alert Logic Addendum

602071 Alert Logic IDS Appliance Tier 1 M- Physical TM4C16GB

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic Intrusion Detection System (IDS) Appliances

An Alert Logic IDS Appliance must be deployed on assets that Client wants to protect with Alert Logic MDR Professional or Alert Logic MDR Essentials. At least one Alert Logic IDS Appliance is required for each environment protected. Alert Logic will provide all appliances.

Physical IDS Appliances (1U rack mounted)

Specification	Supported Bandwidth with Scanning	Supported Bandwidth without Scanning
4 core/16 GB RAM	720 Mbps	1.3 Gbps

Company's Responsibilities and Included Features

Support Services

Monitor Alert Logic IDS appliance health.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Client must provide service resources sufficient to meet the minimum Alert Logic Appliance requirements defined at https://docs.alertlogic.com/requirements/appliance-requirements.htm
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum

602072 Alert Logic IDS Appliance Tier 2 M- Physical TM8C32GB

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert

Logic Addendum.

Alert Logic Intrusion Detection System (IDS) Appliances

An Alert Logic IDS Appliance must be deployed on assets that Client wants to protect with Alert Logic MDR Professional or Alert Logic MDR Essentials. At least one Alert Logic IDS Appliance is required for each environment protected. Alert Logic will provide all appliances.

Physical IDS Appliances (1U rack mounted)

Specification	Supported Bandwidth with Scanning	Supported Bandwidth without Scanning
8 core/32 GB RAM	3.75 Gbps	4.5 Gbps

Company's Responsibilities and Included Features

Support Services

Monitor Alert Logic IDS appliance health.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Client must provide service resources sufficient to meet the minimum Alert Logic Appliance requirements defined at https://docs.alertlogic.com/requirements/appliance-requirements.htm
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum

602073 Alert Logic IDS Appliance Tier 3 M - Physical TM16C64GB

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic Intrusion Detection System (IDS) Appliances

An Alert Logic IDS Appliance must be deployed on assets that Client wants to protect with Alert Logic MDR Professional or Alert Logic MDR Essentials. At least one Alert Logic IDS Appliance is required for each environment protected. Alert Logic will provide all appliances.

Physical IDS Appliances (1U rack mounted)

Specification	Supported Bandwidth with Scanning	Supported Bandwidth without Scanning
16 core/64 GB RAM	10 Gbps	12 Gbps

Company's Responsibilities and Included Features

Support Services

Monitor Alert Logic IDS appliance health.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert

Logic:

- Client must provide service resources sufficient to meet the minimum Alert Logic Appliance requirements defined at https://docs.alertlogic.com/requirements/appliance-requirements.htm
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum

602074 Alert Logic WAF Appliance M - Physical WSM4C16GB

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic WAF Appliances

An Alert Logic WAF Appliance must be deployed on assets that Client wants to protect with Alert Logic Managed WAF. WAF Appliances may be physical or virtual depending upon deployment and service elections. WAF Appliances must be deployed in pairs; high availability/redundancy is required to ensure service consistency. Alert Logic will provide all appliances.

Alert Logic will provide physical WAF Appliances that meet the following specifications:

- 4 Cores
- 16 GB RAM
- 1 RU rack mounted
- 500 GB Disk space
- 250W power supply

602077 Alert Logic WAF Appliance M - Physical WSM8C32GB

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic WAF Appliances

An Alert Logic WAF Appliance must be deployed on assets that Client wants to protect with Alert Logic Managed WAF. WAF Appliances may be physical or virtual depending upon deployment and service elections. WAF Appliances must be deployed in pairs; high availability/redundancy is required to ensure service consistency. Alert Logic will provide all appliances.

Alert Logic will provide physical WAF Appliances that meet the following specifications:

- 8 Cores
- 32 GB RAM
- 1 RU rack mounted
- 500 GB Disk space
- 250W power supply

602078 Alert Logic WAF Appliance M - Physical WSM16C64GB

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic WAF Appliances

An Alert Logic WAF Appliance must be deployed on assets that Client wants to protect with Alert Logic Managed WAF. WAF Appliances may be physical or virtual depending upon deployment and service elections. WAF Appliances must be deployed in pairs; high availability/redundancy is required to ensure service consistency. Alert Logic will provide all appliances.

Alert Logic will provide physical WAF Appliances that meet the following specifications:

- 16 Cores

- 64 GB RAM
- 1 RU rack mounted
- 500 GB Disk space
- 250W power supply

602079 OneNeck Implementation Fee for Alert Logic Services

Company will provide implementation services as defined below in conjunction with managing or reselling Alert Logic, Inc. services and/or products specified herein.

Company's Responsibilities and Included Features

In coordination with the Client, Company will execute the following implementation tasks:

- Discovery of Client environment to create list of nodes for deployment
- Define scope of protection/scanning range by networks and subnets

In coordination with the Client, Company will execute the following implementation tasks for servers, firewalls and other devices managed by Company and used to deploy Alert Logic services:

- Download and install the Alert Logic virtual appliances (or physical if that is the requirement) including setup of appliances and establishment of network connectivity
- Configure firewall/security group access to enable appliance and agent communication including:
    - Opening of firewall ports to communicate with Alert Logic
    - Setup discovery scans in the Alert Logic console
    - Setup vulnerability scanning in the Alert Logic console
- Deploy Alert Logic universal agents for in-scope devices (for collection of network, log data and File Integrity Monitoring (FIM) services)
- Deploy Alert Logic Endpoint Protection agents for in-scope devices
- Install Alert Logic remote log collector and configure included log sources to remote log collector
- Configure network SPAN/TAP port (if needed)
- Configure Event Hub (Azure environments only)
- Configure Alert Logic console as follows:
    - Set up users and notifications in the Alert Logic console
    - Set up correlation policies/alerts in Alert Logic console
    - Set up of initial call and escalation trees

Company will work with Client to make limited configuration adjustments based on the findings from the Alert Logic Deployment Health Review and Incident Tuning Session.

- Depending upon the resources needed to make the configuration adjustments, a separate time and materials statement of work may be required

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Work with Company to provide information as needed for Company to complete its responsibilities as defined above
- Diffie-Hellman traffic cannot be decrypted by Alert Logic s network intrusion detection system (IDS) and thus cannot effectively be monitored; therefore, if Client requires visibility into this traffic with unsupported encryption, remediations will be needed and will require a separate statement of work before Company can proceed

For servers, firewalls and other devices which are not managed by Company and which are used deploy to Alert Logic services, Client is responsible for completion of the following implementation tasks:

- Download and install the Alert Logic virtual appliances (or physical if that is the requirement) including setup of appliances and establishment of network connectivity

- Configure firewall/security group access to enable appliance and agent communication including:
    - Opening of firewall ports to communicate with Alert Logic
    - Setup discovery scans in the Alert Logic console
    - Setup vulnerability scanning in the Alert Logic console
- Deploy Alert Logic universal agents for in-scope devices (for collection of network, log data and File Integrity Monitoring (FIM) services)
- Deploy Alert Logic Endpoint Protection agents for in-scope devices
- Install Alert Logic remote log collector and configure included log sources to remote log collector
- Configure network SPAN/TAP port (if needed)
- Configure Event Hub (Azure environments only)
- Configure Alert Logic console as follows:
    - Set up users and notifications in the Alert Logic console
    - Set up correlation policies/alerts in Alert Logic console
    - Set up of initial call and escalation trees

Category: Alert Logic Resale

601397 Alert Logic MDR Essentials NM - Max Nodes 25

Company will resell Alert Logic, Inc. services and/or products specified herein, for a maximum of 25 Essentials nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Essentials

Alert Logic MDR Essentials is an Alert Logic Hosted Service. Designed to protect low-risk environments that do not contain sensitive data, Alert Logic MDR Essentials provides endpoint detection capabilities and security assessment and posture management.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Essentials
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

A detailed service description of Alert Logic MDR Essentials will be provided to Client upon request.

601398 Alert Logic MDR Essentials NM - Max Nodes 50

Company will resell Alert Logic, Inc. services and/or products specified herein, for a maximum of 50 Essentials nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Essentials

Alert Logic MDR Essentials is an Alert Logic Hosted Service. Designed to protect low-risk environments that do not contain sensitive data, Alert Logic MDR Essentials provides endpoint detection capabilities and security assessment and posture management.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Essentials
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

A detailed service description of Alert Logic MDR Essentials will be provided to Client upon request.

601399 Alert Logic MDR Essentials NM - Max Nodes 100

Company will resell Alert Logic, Inc. services and/or products specified herein, for a maximum of 100 Essentials nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Essentials

Alert Logic MDR Essentials is an Alert Logic Hosted Service. Designed to protect low-risk environments that do not contain sensitive data, Alert Logic MDR Essentials provides endpoint detection capabilities and security assessment and posture management.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning

- Cloud configuration checks
- Endpoint detection

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Essentials
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

A detailed service description of Alert Logic MDR Essentials will be provided to Client upon request.

601400 Alert Logic MDR Essentials NM - Max Nodes 150

Company will resell Alert Logic, Inc. services and/or products specified herein, for a maximum of 150 Essentials nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Essentials

Alert Logic MDR Essentials is an Alert Logic Hosted Service. Designed to protect low-risk environments that do not contain sensitive data, Alert Logic MDR Essentials provides endpoint detection capabilities and security assessment and posture management.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Essentials
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for

monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

A detailed service description of Alert Logic MDR Essentials will be provided to Client upon request.

601401 Alert Logic MDR Essentials NM - Max Nodes 250

Company will resell Alert Logic, Inc. services and/or products specified herein, for a maximum of 250 Essentials nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Essentials

Alert Logic MDR Essentials is an Alert Logic Hosted Service. Designed to protect low-risk environments that do not contain sensitive data, Alert Logic MDR Essentials provides endpoint detection capabilities and security assessment and posture management.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Essentials
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

A detailed service description of Alert Logic MDR Essentials will be provided to Client upon request.

601402 Alert Logic MDR Essentials NM - Max Nodes > 250

Company will resell Alert Logic, Inc. services and/or products specified herein, per Essentials node purchased over 250 Essentials nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Essentials

Alert Logic MDR Essentials is an Alert Logic Hosted Service. Designed to protect low-risk environments that do not contain

sensitive data, Alert Logic MDR Essentials provides endpoint detection capabilities and security assessment and posture management.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Essentials
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

A detailed service description of Alert Logic MDR Essentials will be provided to Client upon request.

601403 Alert Logic MDR Professional NM - Max Nodes 25

Company will resell Alert Logic, Inc. services and/or products as specified herein, for a maximum of 25 Professional nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Professional

Alert Logic MDR Professional is an Alert Logic Hosted Service. Designed to protect environments classified as moderate or high risk, Alert Logic MDR Professional provides fully outsourced 24/7 threat detection for traditional, hybrid, and cloud infrastructures and applications accompanied by actionable guidance to enable customers to quickly respond to attacks.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection
- Network packet monitoring
- Log data monitoring

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Professional
- Alert Logic Remote Log Collector, available under separate ItemID, must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

Log usage for MDR Professional nodes may not exceed an aggregated average of 100 MB/Day/Node in any calendar quarter. Client agrees to pay any and all additional fees that Alert Logic charges for any log usage overages by Client.

A detailed service description of Alert Logic MDR Professional will be provided to Client upon request.

601404 Alert Logic MDR Professional NM - Max Nodes 50

Company will resell Alert Logic, Inc. services and/or products as specified herein, for a maximum of 50 Professional nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Professional

Alert Logic MDR Professional is an Alert Logic Hosted Service. Designed to protect environments classified as moderate or high risk, Alert Logic MDR Professional provides fully outsourced 24/7 threat detection for traditional, hybrid, and cloud infrastructures and applications accompanied by actionable guidance to enable customers to quickly respond to attacks.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection
- Network packet monitoring
- Log data monitoring

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Professional
- Alert Logic Remote Log Collector, available under separate ItemID, must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability

- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

Log usage for MDR Professional nodes may not exceed an aggregated average of 100 MB/Day/Node in any calendar quarter. Client agrees to pay any and all additional fees that Alert Logic charges for any log usage overages by Client.

A detailed service description of Alert Logic MDR Professional will be provided to Client upon request.

601405 Alert Logic MDR Professional NM - Max Nodes 100

Company will resell Alert Logic, Inc. services and/or products as specified herein, for a maximum of 100 Professional nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Professional

Alert Logic MDR Professional is an Alert Logic Hosted Service. Designed to protect environments classified as moderate or high risk, Alert Logic MDR Professional provides fully outsourced 24/7 threat detection for traditional, hybrid, and cloud infrastructures and applications accompanied by actionable guidance to enable customers to quickly respond to attacks.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection
- Network packet monitoring
- Log data monitoring

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Professional
- Alert Logic Remote Log Collector, available under separate ItemID, must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

Log usage for MDR Professional nodes may not exceed an aggregated average of 100 MB/Day/Node in any calendar quarter. Client agrees to pay any and all additional fees that Alert Logic charges for any log usage overages by Client.

A detailed service description of Alert Logic MDR Professional will be provided to Client upon request.

601406 Alert Logic MDR Professional NM - Max Nodes 150

Company will resell Alert Logic, Inc. services and/or products as specified herein, for a maximum of 150 Professional nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Professional

Alert Logic MDR Professional is an Alert Logic Hosted Service. Designed to protect environments classified as moderate or high risk, Alert Logic MDR Professional provides fully outsourced 24/7 threat detection for traditional, hybrid, and cloud infrastructures and applications accompanied by actionable guidance to enable customers to quickly respond to attacks.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection
- Network packet monitoring
- Log data monitoring

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Professional
- Alert Logic Remote Log Collector, available under separate ItemID, must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

Log usage for MDR Professional nodes may not exceed an aggregated average of 100 MB/Day/Node in any calendar quarter. Client agrees to pay any and all additional fees that Alert Logic charges for any log usage overages by Client.

A detailed service description of Alert Logic MDR Professional will be provided to Client upon request.

601407 Alert Logic MDR Professional NM - Max Nodes 250

Company will resell Alert Logic, Inc. services and/or products as specified herein, for a maximum of 250 Professional nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Professional

Alert Logic MDR Professional is an Alert Logic Hosted Service. Designed to protect environments classified as moderate or high

risk, Alert Logic MDR Professional provides fully outsourced 24/7 threat detection for traditional, hybrid, and cloud infrastructures and applications accompanied by actionable guidance to enable customers to quickly respond to attacks.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection
- Network packet monitoring
- Log data monitoring

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Professional
- Alert Logic Remote Log Collector, available under separate ItemID, must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

Log usage for MDR Professional nodes may not exceed an aggregated average of 100 MB/Day/Node in any calendar quarter. Client agrees to pay any and all additional fees that Alert Logic charges for any log usage overages by Client.

A detailed service description of Alert Logic MDR Professional will be provided to Client upon request.

601408 Alert Logic MDR Professional NM - Max Nodes 500

Company will resell Alert Logic, Inc. services and/or products as specified herein, for a maximum of 500 Professional nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Professional

Alert Logic MDR Professional is an Alert Logic Hosted Service. Designed to protect environments classified as moderate or high risk, Alert Logic MDR Professional provides fully outsourced 24/7 threat detection for traditional, hybrid, and cloud infrastructures and applications accompanied by actionable guidance to enable customers to quickly respond to attacks.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection
- Network packet monitoring

- Log data monitoring

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Professional
- Alert Logic Remote Log Collector, available under separate ItemID, must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

Log usage for MDR Professional nodes may not exceed an aggregated average of 100 MB/Day/Node in any calendar quarter. Client agrees to pay any and all additional fees that Alert Logic charges for any log usage overages by Client.

A detailed service description of Alert Logic MDR Professional will be provided to Client upon request.

601409 Alert Logic MDR Professional NM - Max Nodes 750

Company will resell Alert Logic, Inc. services and/or products as specified herein, for a maximum of 1,000 Professional nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Professional

Alert Logic MDR Professional is an Alert Logic Hosted Service. Designed to protect environments classified as moderate or high risk, Alert Logic MDR Professional provides fully outsourced 24/7 threat detection for traditional, hybrid, and cloud infrastructures and applications accompanied by actionable guidance to enable customers to quickly respond to attacks.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection
- Network packet monitoring
- Log data monitoring

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Professional

- Alert Logic Remote Log Collector, available under separate ItemID, must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

Log usage for MDR Professional nodes may not exceed an aggregated average of 100 MB/Day/Node in any calendar quarter. Client agrees to pay any and all additional fees that Alert Logic charges for any log usage overages by Client.

A detailed service description of Alert Logic MDR Professional will be provided to Client upon request.

601410 Alert Logic MDR Professional NM - Max Nodes 1000

Company will provide support services as defined below in conjunction with reselling Alert Logic, Inc. services and/or products specified herein, for a maximum of 1,000 Professional nodes.

Alert Logic, Inc. services and/or products are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Professional

Alert Logic MDR Professional is an Alert Logic Hosted Service. Designed to protect environments classified as moderate or high risk, Alert Logic MDR Professional provides fully outsourced 24/7 threat detection for traditional, hybrid, and cloud infrastructures and applications accompanied by actionable guidance to enable customers to quickly respond to attacks.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection
- Network packet monitoring
- Log data monitoring

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Professional
- Alert Logic Remote Log Collector, available under separate ItemID, must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic

s EULA (End User License Agreement)

Log usage for MDR Professional nodes may not exceed an aggregated average of 100 MB/Day/Node in any calendar quarter. Client agrees to pay any and all additional fees that Alert Logic charges for any log usage overages by Client.

A detailed service description of Alert Logic MDR Professional will be provided to Client upon request.

601411 Alert Logic MDR Professional NM - Max Nodes > 1000

Company will resell Alert Logic, Inc. services and/or products as specified herein, per Professional node purchased over 1,000 Professional nodes.

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Professional

Alert Logic MDR Professional is an Alert Logic Hosted Service. Designed to protect environments classified as moderate or high risk, Alert Logic MDR Professional provides fully outsourced 24/7 threat detection for traditional, hybrid, and cloud infrastructures and applications accompanied by actionable guidance to enable customers to quickly respond to attacks.

Key Features include:

- Asset discovery
- Internal and external vulnerability scanning
- Cloud configuration checks
- Endpoint detection
- Network packet monitoring
- Log data monitoring

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Alert Logic IDS Appliance Virtual or Physical, available under separate ItemID, must be deployed on any assets desired to be protected by Alert Logic MDR Professional
- Alert Logic Remote Log Collector, available under separate ItemID, must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic
- Infrastructure configuration, installation and setup of Alert Logic physical or virtual appliances (as applicable), configuration for appliance and agent communication, deployment of Alert Logic agents and Alert Logic console configuration
- Designate a primary Client contact to be the point of contact for Alert Logic escalation for security issues
- Monitor for backend application availability
- Provide accurate and up-to-date SSL certificates and keys (required for Alert Logic to tune or configure its products for monitoring and protection of HTTPS traffic)
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum, including but not limited to Alert Logic s EULA (End User License Agreement)

Log usage for MDR Professional nodes may not exceed an aggregated average of 100 MB/Day/Node in any calendar quarter. Client agrees to pay any and all additional fees that Alert Logic charges for any log usage overages by Client.

A detailed service description of Alert Logic MDR Professional will be provided to Client upon request.

601412 Alert Logic Setup Fee

Alert Logic will assist the Client throughout the implementation of Alert Logic MDR Professional services purchased under this SOW.

Alert Logic will assign a member of its project management team as Client s single point of contact to implement the Alert Logic MDR Professional services and will coordinate with the Client on the deployment of all services.

Client's Responsibilities and Out-of-Scope Notes

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Agent Installation
  - Installing agents
  - Configuring appropriate firewall access to enable agent communication
  - Configuring appropriate access to enable appliance communication
  - Notifying Alert Logic when installation of agents is complete
- Appliance Installation - On Premises
  - Racking and installing the physical appliance(s), and/or loading and installing the virtual appliance image
  - Providing network access to the appliance(s) for Alert Logic personnel
  - Configuring appropriate firewall access to enable appliance communication
  - Notifying Alert Logic when installation of the appliance(s) is complete
- Appliance Installation - In Cloud
  - Configuring appropriate Security Group access to enable appliance communication
- Technical Deployment
  - Provisioning of appropriate technical resources and information during deployment
  - Technical resources are required to attend the project Kick Off and orientation sessions and to carry out project activity required to establish the service during the deployment project, including following the training curriculum
  - Technical resources are required to provide information and context about the Client environment to enrich the service
- Operational Integration
  - Provisioning of appropriate operational resources and information during the deployment project
  - Client operational resources are required to carry out integration activity to ensure the transition is ready to consume the Alert Logic services, attend service orientation, and complete the training curriculum

601413 Alert Logic Managed WAF NM 1-5 Websites

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic Managed WAF

Alert Logic Managed WAF (Web Application Firewall) is an Alert Logic Hosted Service that provides inline web application protection by detecting and blocking potential threats from reaching Client web applications. The Alert Logic Managed WAF service includes ActiveWatch. Alert Logic ActiveWatch leverages Alert Logic ActiveIntelligence, ActiveAnalytics, Data Science Experts, Web Application Security Experts and the Security Analysts in Alert Logic s Security Operations Centers to provide application policy configuration, tuning and guidance.

Minimum Appliance Requirements

- An Alert Logic WAF Appliance must be deployed on assets that Client wants to protect with Alert Logic Managed WAF
- WAF Appliances may be physical or virtual depending upon deployment and service elections
- WAF Appliances must be deployed in pairs; high availability/redundancy is required to ensure service consistency

A detailed service description of Alert Logic Managed WAF will be provided to Client upon request.

601414 Alert Logic Managed WAF NM 6-10 Websites

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic Managed WAF

Alert Logic Managed WAF (Web Application Firewall) is an Alert Logic Hosted Service that provides inline web application protection by detecting and blocking potential threats from reaching Client web applications. The Alert Logic Managed WAF service includes ActiveWatch. Alert Logic ActiveWatch leverages Alert Logic ActiveIntelligence, ActiveAnalytics, Data Science Experts, Web Application Security Experts and the Security Analysts in Alert Logic s Security Operations Centers to provide application policy configuration, tuning and guidance.

Minimum Appliance Requirements

- An Alert Logic WAF Appliance must be deployed on assets that Client wants to protect with Alert Logic Managed WAF
- WAF Appliances may be physical or virtual depending upon deployment and service elections
- WAF Appliances must be deployed in pairs; high availability/redundancy is required to ensure service consistency

A detailed service description of Alert Logic Managed WAF will be provided to Client upon request.

601415 Alert Logic Managed WAF NM Additional Websites

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic Managed WAF

Alert Logic Managed WAF (Web Application Firewall) is an Alert Logic Hosted Service that provides inline web application protection by detecting and blocking potential threats from reaching Client web applications. The Alert Logic Managed WAF service includes ActiveWatch. Alert Logic ActiveWatch leverages Alert Logic ActiveIntelligence, ActiveAnalytics, Data Science Experts, Web Application Security Experts and the Security Analysts in Alert Logic s Security Operations Centers to provide application policy configuration, tuning and guidance.

Minimum Appliance Requirements

- An Alert Logic WAF Appliance must be deployed on assets that Client wants to protect with Alert Logic Managed WAF
- WAF Appliances may be physical or virtual depending upon deployment and service elections
- WAF Appliances must be deployed in pairs; high availability/redundancy is required to ensure service consistency

A detailed service description of Alert Logic Managed WAF will be provided to Client upon request.

601422 Alert Logic MDR Enterprise NM

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic MDR Enterprise

Alert Logic MDR Enterprise is an Alert Logic Hosted Service that augments the Alert Logic MDR Professional Service. An Alert Logic security analyst is assigned to the Client who will develop knowledge of the Client s security environment to enable recommendations for continual advancement in Client s security posture.

Key Features include:

- Continuous threat hunting
- Proactive tuning and sensor optimization
- Extended security investigations
- Weekly security review

Annual on-site

Minimum Requirements

Client must purchase and maintain an Alert Logic MDR Professional service to add the Alert Logic MDR Enterprise service.

A detailed service description of Alert Logic MDR Enterprise will be provided to Client upon request.

601425 Alert Logic IDS Appliance NM - Virtual

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic Intrusion Detection System (IDS) Appliances

An Alert Logic IDS Appliance must be deployed on assets that Client wants to protect with Alert Logic MDR Professional or Alert Logic MDR Essentials. At least one Alert Logic IDS Appliance is required for each environment protected. Alert Logic will provide all appliances.

System Requirements for Virtual IDS Appliances

Virtual CPU Cores	Components	System Requirements
4 cores	RAM	16 GB
4 cores	Disk space	40 GB Minimum
4 cores	Supported virtual environment	VMware, Hyper-V, AHV
4 cores	Encryption	TLS Standard (SSL): 2048-bit key encryption, 256-bit AES bulk encryption
4 cores	Peak supported throughput	500 Mbps
8 cores	RAM	32 GB
8 cores	Disk space	40 GB Minimum
8 cores	Supported virtual environment	VMware, Hyper-V, AHV
8 cores	Encryption	TLS Standard (SSL): 2048-bit key encryption, 256-bit AES bulk encryption
8 cores	Peak supported throughput	1 Gbps
16 cores	RAM	64 GB
16 cores	Disk space	40 GB Minimum
16 cores	Supported virtual environment	VMware, Hyper-V, AHV
16 cores	Encryption	TLS Standard (SSL): 2048-bit key encryption, 256-bit AES bulk encryption
16 cores	Peak supported throughput	2 Gbps (1 Gbps per fiber interface)

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Client must provide virtual service resources sufficient to meet the minimum Alert Logic Virtual Appliance requirements defined at https://docs.alertlogic.com/requirements/appliance-requirements.htm
- Client is responsible for installing and configuring the virtual Alert Logic IDS appliance in accordance with Alert Logic s

installation instructions available at https://docs.alertlogic.com/prepare/virtual-appliance.htm

- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum

601426 Alert Logic WAF Appliance NM - Virtual

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic WAF Appliances

An Alert Logic WAF Appliance must be deployed on assets that Client wants to protect with Alert Logic Managed WAF. WAF Appliances may be physical or virtual depending upon deployment and service elections. WAF Appliances must be deployed in pairs; high availability/redundancy is required to ensure service consistency. Alert Logic will provide all appliances.

System Requirements for Virtual WAF Appliances

Components	**System Requirements**
CPU	2 CPUs 64 bit
RAM	4 GB
Disk space	250 GB
Virtual network interface(s)	An interface with an external IP address for management; an interface with access to the web servers to be protected
Encryption/Decryption for SSL traffic	AES-NI CPU instruction set for encryption/decryption of SSL traffic on VMs and host OS is recommended
Clustering	For clustering to work, ensure promiscuous mode, forged transmits, and MAC address changes are allowed on the VMware virtual switch (vSwitch) or the port group in the VMware ESX network configuration

601427 Alert Logic Log Collector NM - Linux

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic Remote Log Collector

With Alert Logic MDR Professional Services, an Alert Logic remote log collector must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic. The Alert Logic syslog remote collector agent software is installed on a VMware Windows server dedicated to the collection of syslog data.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Client must provide virtual infrastructure and a Linux virtual machine/server to run the remote log collector VM

Fulfill Client responsibilities outlined within the attached Alert Logic Addendum

601428 Alert Logic IDS Appliance Tier 1 NM - Physical TM4C16GB

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic Intrusion Detection System (IDS) Appliances

An Alert Logic IDS Appliance must be deployed on assets that Client wants to protect with Alert Logic MDR Professional or Alert Logic MDR Essentials. At least one Alert Logic IDS Appliance is required for each environment protected. Alert Logic will provide all appliances.

Physical IDS Appliances (1U rack mounted)

Specification	Supported Bandwidth with Scanning	Supported Bandwidth without Scanning
4 core/16 GB RAM	720 Mbps	1.3 Gbps

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Client must provide service resources sufficient to meet the minimum Alert Logic Appliance requirements defined at https://docs.alertlogic.com/requirements/appliance-requirements.htm
- Client is responsible for installing and configuring the Alert Logic IDS appliance in accordance with Alert Logic s installation instructions available at https://docs.alertlogic.com/prepare/alert-logic-physical-appliance.htm
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum

601429 Alert Logic IDS Appliance Tier 2 NM - Physical TM8C32GB

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic Intrusion Detection System (IDS) Appliances

An Alert Logic IDS Appliance must be deployed on assets that Client wants to protect with Alert Logic MDR Professional or Alert Logic MDR Essentials. At least one Alert Logic IDS Appliance is required for each environment protected. Alert Logic will provide all appliances.

Physical IDS Appliances (1U rack mounted)

Specification	Supported Bandwidth with Scanning	Supported Bandwidth without Scanning
8 core/32 GB RAM	3.75 Gbps	4.5 Gbps

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Client must provide service resources sufficient to meet the minimum Alert Logic Appliance requirements defined at https://docs.alertlogic.com/requirements/appliance-requirements.htm
- Client is responsible for installing and configuring the Alert Logic IDS appliance in accordance with Alert Logic s installation instructions available at https://docs.alertlogic.com/prepare/alert-logic-physical-appliance.htm
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum

601430 Alert Logic IDS Appliance Tier 3 NM - Physical TM16C64GB

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic Intrusion Detection System (IDS) Appliances

An Alert Logic IDS Appliance must be deployed on assets that Client wants to protect with Alert Logic MDR Professional or Alert Logic MDR Essentials. At least one Alert Logic IDS Appliance is required for each environment protected. Alert Logic will provide all appliances.

Physical IDS Appliances (1U rack mounted)

Specification	Supported Bandwidth with Scanning	Supported Bandwidth without Scanning
16 core/64 GB RAM	10 Gbps	12 Gbps

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Client must provide service resources sufficient to meet the minimum Alert Logic Appliance requirements defined at https://docs.alertlogic.com/requirements/appliance-requirements.htm
- Client is responsible for installing and configuring the Alert Logic IDS appliance in accordance with Alert Logic s installation instructions available at https://docs.alertlogic.com/prepare/alert-logic-physical-appliance.htm
- Fulfill Client responsibilities outlined within the attached Alert Logic Addendum

601431 Alert Logic WAF Appliance NM - Physical WSM4C16GB

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic WAF Appliances

An Alert Logic WAF Appliance must be deployed on assets that Client wants to protect with Alert Logic Managed WAF. WAF Appliances may be physical or virtual depending upon deployment and service elections. WAF Appliances must be deployed in pairs; high availability/redundancy is required to ensure service consistency. Alert Logic will provide all appliances.

Alert Logic will provide physical WAF Appliances that meet the following specifications:

- 4 Cores
- 16 GB RAM
- 1 RU rack mounted
- 500 GB Disk space
- 250W power supply

601432 Alert Logic WAF Appliance NM - Physical WSM8C32GB

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic WAF Appliances

An Alert Logic WAF Appliance must be deployed on assets that Client wants to protect with Alert Logic Managed WAF. WAF Appliances may be physical or virtual depending upon deployment and service elections. WAF Appliances must be deployed in pairs; high availability/redundancy is required to ensure service consistency. Alert Logic will provide all appliances.

Alert Logic will provide physical WAF Appliances that meet the following specifications:

- 8 Cores
- 32 GB RAM
- 1 RU rack mounted
- 500 GB Disk space
- 250W power supply

601433 Alert Logic WAF Appliance NM - Physical WSM16C64GB

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic WAF Appliances

An Alert Logic WAF Appliance must be deployed on assets that Client wants to protect with Alert Logic Managed WAF. WAF Appliances may be physical or virtual depending upon deployment and service elections. WAF Appliances must be deployed in pairs; high availability/redundancy is required to ensure service consistency. Alert Logic will provide all appliances.

Alert Logic will provide physical WAF Appliances that meet the following specifications:

- 16 Cores
- 64 GB RAM
- 1 RU rack mounted
- 500 GB Disk space
- 250W power supply

601732 Alert Logic Log Collector NM - Windows

The services and/or products as defined under this ItemID are provided subject to, and in accordance with, the attached Alert Logic Addendum.

Alert Logic Remote Log Collector

With Alert Logic MDR Professional Services, an Alert Logic remote log collector must be deployed to collect, compress and encrypt syslog data to send directly to Alert Logic. The Alert Logic syslog remote collector agent software is installed on a VMware Windows server dedicated to the collection of syslog data.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Unless otherwise covered by another ItemID in this SOW or a separate agreement with Company or Alert Logic, Client shall be responsible for the following activities, which shall be deemed outside the scope of services provided by Company or Alert Logic:

- Client must provide virtual infrastructure and a Windows virtual machine/server to run the remote log collector VM

Fulfill Client responsibilities outlined within the attached Alert Logic Addendum

Category: Managed Applications

302159 Hosted Exchange 2010 Standard: Advanced Plan Mailbox

Company's Responsibilities and Included Features

- User mailbox for email, calendar, contacts
- Collaborative environment to share calendars, contacts, and notes

Outlook web application for secure "anywhere" access

- Unlimited user storage
- Includes Active Directory sync
- Online knowledge base
- Activesync for iPhone, iPad, Android and other mobile devices
- SpamStopper Pro (antivirus, antispam)
- Daily snapshots are taken of the Exchange environment and retained for 7 days
- 1 Public folder per account
- Client disclaimer (per account)
- 1 Resource mailbox
- Compliant archiving enablement (per account)
- MessageMirror archiving with 25 GB of storage (per account)
- SharePoint Foundation 2010 with 1 GB of storage
- 1 GB of Outlook backup storage (for PST's) included (per user) with retention period of 7 days
- 50 Fax-via-email pages included
- Onboarding migration included (migration from Notes or GroupWise are additional costs)
- Off-boarding migration assistance included (migration to Notes or GroupWise are additional costs)
- 50 domains included
- Maximum Client contacts: 5,000
- Maximum distribution lists: 1,000
- Maximum message size: 50MB
- Maximum recipients per message: 500
- No charge for split domain
- Point in time restore of mailbox data at additional cost
- 99.999% uptime guarantee (unless otherwise excluded in the pricing or service level commitments)
- This is a metered service and will be billed monthly based on actual subscribed quantities.

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Self-management the Exchange environment
- Blackberry sync
- End user support

500018 Message Encryption (per user)

Company's Responsibilities and Included Features

- Policy based message encryption

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- End user support

603869 Platinum - IT Complete Support and Management

Company's Responsibilities and Included Features

Company's responsibilities for this service are defined in the Platinum Information Services inc. Professional Services Proposal and Agreement, Appendix A

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Client's responsibilities are defined in the Platinum Information Services inc. Professional Services Proposal and Agreement, Appendix A

Category: Megaport

606803 Megaport Port Service

Company s Responsibilities and Included Features

Megaport Port Service

The Megaport Port Service provides for connectivity services to the Megaport network with technical specifications detailed in the Megaport site documentation https://docs.megaport.com/tech-specs/.

Megaport s services are comprised of fixed and consumption-based service components that will be measured, and billing based on Client s usage within the billing period.

Client s Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Acknowledgement and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of this offering is by Megaport (USA), Inc., and may be subject to changes in provisioning and performance as determined by Megaport (USA), Inc.
- Client agrees that Megaport (USA), Inc. offerings provided herein are subject to the terms of Megaport s Global Services Agreement located at https://www.megaport.com/legal/, which is hereby incorporated into this SOW in full.

606804 Megaport Virtual Cross Connect (VXC) Service

Company s Responsibilities and Included Features

VXC (Virtual Cross Connect)

The Virtual Cross Connect allows for connection to services on the Megaport network. Details and technical specifications of the Virtual Cross Connects can be found on the Megaport site documentation https://docs.megaport.com/connections/.

Megaport s services are comprised of fixed and consumption-based service components that will be measured, and billing based on Client s usage within the billing period.

Client s Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Acknowledgement and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of this offering is by Megaport (USA), Inc., and may be subject to changes in provisioning and performance as determined by Megaport (USA), Inc.
- Client agrees that Megaport (USA), Inc. offerings provided herein are subject to the terms of Megaport s Global Services Agreement located at https://www.megaport.com/legal/, which is hereby incorporated into this SOW in full.

606805 Megaport Cloud Router (MCR) Service

Company s Responsibilities and Included Features

MCR (Megaport Cloud Router)

The Megaport Cloud Router provides for a managed virtual router service for connectivity on the Megaport software-defined network. Technical details and specifications are available on the Megaport site documentation https://docs.megaport.com/mcr/.

Megaport s services are comprised of fixed and consumption-based service components that will be measured, and billing based on Client s usage within the billing period.

Client s Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Acknowledgement and EULA

Client agrees, acknowledges, and understands that the actual manufacture of this offering is by Megaport (USA), Inc., and may be subject to changes in provisioning and performance as determined by Megaport (USA), Inc.
- Client agrees that Megaport (USA), Inc. offerings provided herein are subject to the terms of Megaport s Global Services Agreement located at https://www.megaport.com/legal/, which is hereby incorporated into this SOW in full.

606806 Megaport Virtual Edge (MVE) Service

Company s Responsibilities and Included Features

MVE (Megaport Virtual Edge)

The Megaport Virtual Edge provides virtual infrastructure for network services at the edge of Megaport s software-defined network. Details and technical specifications of MVE can be found on Megaport s site documentation https://docs.megaport.com/mve/.

Megaport s services are comprised of fixed and consumption-based service components that will be measured, and billing based on Client s usage within the billing period.

Client s Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

Acknowledgement and EULA

- Client agrees, acknowledges, and understands that the actual manufacture of this offering is by Megaport (USA), Inc., and may be subject to changes in provisioning and performance as determined by Megaport (USA), Inc.
- Client agrees that Megaport (USA), Inc. offerings provided herein are subject to the terms of Megaport s Global Services Agreement located at https://www.megaport.com/legal/, which is hereby incorporated into this SOW in full.

Category: NDS Managed Network

604362 Network Data Systems Managed Aruba Switch

Company's Responsibilities and Included Features

Remote Managed Service (RMS) for Client Premise Equipment (CPE) is provided by Network Data Systems, Inc. (NDS) through the NDS Network Operation Center (NOC) in accordance with the Network Data Systems Addendum to the Statement of Work. This SKU provides for the hardware management of Aruba switches through the NDS NOC RMS.

Remote Managed NOC Services (RMS)

- In the event there is a site related issue (loss of power to site, damage to premise cabling, accidental disconnection of cabling or equipment, or carrier issues) that causes an outage of devices or systems under management, the NOC will document the issue within the NOC ticketing system, notify the Expert User(s), and manage the issue until resolution. The NOC will close the ticket once the site related issue is remediated. When the ticket is closed, the Clients designated contact will receive an email indicating that the site issue is resolved
- If a contracted device has a component hardware failure, the NOC will diagnose and attempt to resolve the issue remotely. If the hardware failure cannot be resolved remotely, the NOC will begin dispatch of a replacement part (via the Clients vendor maintenance support contract) when needed
- 24x7x365 device and circuit monitoring to include real-time polling of devices
- Detection, isolation, diagnosis of each fault and restoration to normal operating conditions
- Testing and documenting each fault within the NOC ticketing system
- Ownership of resolution of the problem on behalf of the Clients
- Act as an agent for the Client under executed letters of agency
- Expert User(s) notification of the progress of all faults per the Client provided contact(s) and escalation process
- Safeguard Client's proprietary information
- Take all necessary precautions to ensure a secure connection from the NOC into the Clients network
- Secure Expert User(s) web portal access to

View the fault management alarms and event logs
    - Open tickets
    - View contact information

Fault Monitoring

- For each managed device, NOC will monitor up to 10 critical interfaces as identified by the Client during on-boarding. Additional interfaces can be added for an additional fee
- Event Log Montioring - If a critical event occurs the NOC monitoring tools sends out an alert and the NOC will notify the Expert User(s) of the alarm
- Trap Monitoring - The NOC can configure the traps to send critical event information to the network monitoring tools that can create alarms to trigger a trouble ticket
- Problem Identification and Triage - The NOC will notify the Expert User(s). The Service will document the NOC and Expert User(s) acitvities to remediate the isseu and report when the issue has been corrected

Fault Management

- Fault - A fault is defined as a failed device poll indicating the target device is not visible to the NOC network management systems and tools
- If a critical task or function turns off, the NOC will open a ticket and troubleshoot the alarm and resolve the issue. When a fault is identified, the NOC will take ownership of the issue until it is resolved
- The NOC will open a ticket and troubleshoot the cause of alarms. When the cause of the alarm is confirmed, the NOC will resolve the issue
- If the NOC cannot fix the issue directly, the NOC will open a ticket with the vendor (under a vendor maintenance support contract) and work with the vendor support team to resolve the issue, taking ownership until the issue is resolved
- The NOC can configure the traps to send event information to the network monitoring tools, which can trigger a trouble ticket

Configuration Management

- This service provides Access Control giving NOC secure and quick remote access to the managed equipment and keeps an audit trail of who has logged into the client system and when logins occur
- RMS Equipment Configuration Management responsibilities
    - Maintain a log of network device configuration changes
    - Daily polling of each contracted network device to determine if configuration changes have occurred
    - Tracking and archiving of configuration
    - Capturing and archiving the most recent 30 device configuration changes
    - Rapid recovery in the event of configuration loss or changes, or performance issues

Performance and Patch Management

- The NOC monitoring tools measure performance benchmarks of managed network devices to identify and resolve performance bottlenecks in the Client s system
    - The NOC and Expert User(s) must mutually agree on the settings for performance thresholds of all devices
    - The NOC notifies the Expert User(s) when agreed upon device performance thresholds have been exceeded
    - Settings will be evaluated after 90 days of recorded remote monitoring
- Patch Management - The NOC will provide Remote Critical Patch Updates for managed CPE systems
- The NOC will Inform the Expert User(s) about:
    - Critical updates and their availability
    - Current configuration and operational status of the Client devices affected
    - Potential issues with the updates
    - Hardware requirements that for implementing upgrades
- The NOC will perform the remote patch update installation via remote access in accordance with the Client s management processes
- NOC Service includes patch management of 1 patch per quarter, per device or a total of 4 per year. Additional patch management can be supported with professional service hours

- The NOC will periodically review the managed environment and benchmark the environment s performance against NOC optimization standards
- If the NOC recommends any performance improvements, Expert User(s) will be notified in the periodic business review

Device Vendor Management

- The NOC will manage vendors (thru letters of agency) for:
- Replacement parts dispatch thru manufacturer maintenance contracts
- Replacement parts dispatch thru manufacturer maintenance contracts with on-site technician parts replacement
- Incident management with Telco's WAN
- Vendor tickets

Remote Technical Support

- The NOC will work with the hardware vendor (thru letter of authorization) on the Clients behalf to expedite replacement of defective parts. All managed devices are required to have a vendor maintenance contract to provide replacement parts
- The NOC will receive calls from the Expert User(s) or internal IT group after a problem has been identified
- Once a problem has been identified, the NOC will attempt to resolve the issue remotely (i.e., working with Client as needed). If the issue is hardware related, the NOC will open a trouble ticket with the appropriate hardware vendor (under an executed Letter of Agency) and work the problem through resolution

On-site Maintenance

- If on-site device replacement is required, a vendor maintenance contract (with on-site replacement) will need to be purchased by the Client
    - In lieu of an on-site engineer supplied by the NOC, arrangements will have to be made to supply the NOC with an Expert User(s) to provide physical support on-site as directed by the NOC

Support Severity Level Summary

Fault ID	Objective Description	Service Level Response
S1	Detection of Severity 1 (S1) events on the Client network	Within 15 Minutes
S2	Detection of Severity 2 (S2) events on the Client network	Within 15 Minutes
S3	Detection of Severity 3 (S3) events on the Client network	Within 1 hour
S4	Detection of Severity 4 (S4) events on the Client network	Within 2 Business Days

Support Level Definition

(S1) - Critical Severity:

- Produces an emergency in which the network is inoperable, produces incorrect results, or fails catastrophically, or a mainline function of the network is inoperative (i.e., a critical application server), causing significant impact on the Clients business operations (i.e., the Clients production network is down causing critical impact to business operations if service is not restored quickly)
- The NOC and the Client are willing to commit full-time resources around the clock to resolve the situation

(S2) - High Severity:

- Produces a situation in which the network is inoperable, produces incorrect results, or a mainline function of the network is inoperative (i.e., a critical application server), causing a major impact on the Clients business operations (i.e., the Clients production network is severely degraded, impacting significant aspects of business operations)
- The NOC and the Client are willing to commit full-time resources during business hours to resolve the situation

(S3) - Medium Severity:

- Produces a non-critical situation in which the network produces incorrect results, or a feature of the network is inoperative, causing a minor impact on the Client business operations (i.e., the Clients network performance is degraded; network functionality is noticeably impaired, but most business operations continue)

- The NOC shall make commercially reasonable efforts to resolve the problem or provide a workaround as agreed upon between the parties

(S4) - Low Severity:

- General questions, MACD requests and/or inquiries causing little or no impact on the Clients business operations
- The remote management services make commercially reasonable efforts to resolve the problem or provide a workaround as agreed upon between the parties

Device Count Reconciliation

- NOC will conduct a regular audit of total device counts
- Inventory will be compared to the original contract of managed devices to determine if any additions or deletions to the original device count have occurred
- If the number of devices (access point, controller, switches, router, server, etc.) exceed the original contract, the monthly fee will be adjusted
- NOC will onboard all new devices found during the audit and will monitor devices until they are in stable condition and ready for support prior to taking over management
- If issues are discovered during the 2-week period after onboarding a device, NOC will report to the Client/installer to agree on remediation efforts prior to monitoring support beginning. These remediation efforts will be deemed as outside of normal RMS responsibilities and thus will consume professional services hours
- If a device is not able to be successfully on-boarded due to issues, the Client will not be charged the on-boarding fee and the device will be removed from the NOC monitoring systems

Device(s) added after the initial on-boarding will incur a $50 setup fee for each device to cover administrative costs of adding devices to systems and testing connectivity.

Reports

- NOC will provide reports for Expert User(s) about the state of the managed CPE and Applications
- Weekly Reports - These reports look at summarizing the weekly ticket activity showing all tickeets opened, closed and still active tickets
- Monthly Reports - These monthly reports look at the contracted infrastructure devices. The reports include statistics on:
    - Network, device uptime and availability
    - Fault history
    - Trouble tickets
    - Professional Services hours used

Strategic Reporting

- Periodic Business Review - Provides business intelligence information based on the data that the NOC gathers during the period under review. This information has potential business impacting information that reflects
- CPE network trends observed
- Capacity planning
- Resource utilization trends
- Ticketing trends
- Compliance issues
- Normal operating specifications
- Security concerns and business continuity planning
- The goal of this report is to:
    - Characterize the existing managed environment
    - Make specific recommendations for improvement
    - Trouble tickets
    - Provide budgetary information to implement the recommendations

Report-based recommendations

- Immediate Impact recommendations provide an immediate impact on performance across the managed network

- High Impact recommendations provide additional improvements in performance as well as increasing network management efficiency
- Strategic recommendations focus on ensuring that the network will scale to meet future business requirements and that the Client will be able to proactively monitor and manage network performance using the NOC
- Performance Analysis - Provides information about the overall performance of the managed network showing
    - Bottlenecks
    - Areas of high utilization
    - Areas of under-utilization
    - Dropped packets
    - Unusually high error rates
    - Lower than normal device uptime

Report-based recommendations

- Triage of network device incidents
- Troubleshoot and work to resolve network device incidents
- Document network device errors

Move, Add, Change, Deletes (MACD)

- MACD is provided under a separate ItemID. See ItemID 604367.

Professional Services Block of Hours

- A Professional Services Block of Hours is provided under a separate ItemID. See ItemID 604366.

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

- Those defined as Expert Users will be forward to NDS as Customer Designated Contacts

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Client must have contracted for MACD and Professional Services
- Only Expert User(s) should call the NOC directly to ask questions regarding use of the servers, applications, features or capabilities
- All managed devices are required to have a vendor maintenance contract to provide replacement parts

Out of Scope Activities

- Staging, configuring, and installing equipment for non- break fix related issues
- System re-configuration to support product replacement of CPE or for non-break fix issues (Examples may include, but are not limited to, replacing devices due to end of life or end of support or replacement of devices for convenience.) These requests can be supported with extend support hours or as a separate project
- Major re-configuration activities to support non-break fix activities (not including MACD)
- Creation of custom reporting
- General help desk support for users not defined as Expert Users
- Updating of Client workstations or mobile devices to meet policy-based requirements

- Creation of firewall configuration and security policies
- Supporting Client PC, laptops, or mobile devices for non-connectivity issues (including, but not limited to, device application issues or device OS/IOS issues)
- Supporting third party applications that are not defined as part of the NOC
- Monitoring and management of Client CPE (routers, switches, or other devices) not defined in the Service Initiation Form
- Onsite NOC support, unless Onsite Remote Managed (OMS) service option is selected
- Client access to conductor or orchestration service platform
- NOC assumes no liability for security breaches, security policies, denial of service incidents, or other related security incidents
- Remediation of production issues on the current infrastructure
- Optimization or re-configuration activities for current infrastructure
- Equipment staging services for solution devices and equipment
- Network and firewall configuration support for current infrastructure to enable services
- Troubleshooting Client applications traversing service
- On-site support for equipment installation and project services
- Assessment or site survey services to conduct discovery of Client s current network and application environment
- Decommissioning and removal of any existing customer owned equipment in not within the scope of this engagement

604363 Network Data Systems Managed Aruba Router

Company's Responsibilities and Included Features

Remote Managed Service (RMS) for Client Premise Equipment (CPE) is provided by Network Data Systems, Inc. (NDS) through the NDS Network Operation Center (NOC) in accordance with the Network Data Systems Addendum to the Statement of Work. This SKU provides for the hardware management of Aruba routers through the NDS NOC RMS.

Remote Managed NOC Services (RMS)

- In the event there is a site related issue (loss of power to site, damage to premise cabling, accidental disconnection of cabling or equipment, or carrier issues) that causes an outage of devices or systems under management, the NOC will document the issue within the NOC ticketing system, notify the Expert User(s), and manage the issue until resolution. The NOC will close the ticket once the site related issue is remediated. When the ticket is closed, the Clients designated contact will receive an email indicating that the site issue is resolved
- If a contracted device has a component hardware failure, the NOC will diagnose and attempt to resolve the issue remotely. If the hardware failure cannot be resolved remotely, the NOC will begin dispatch of a replacement part (via the Clients vendor maintenance support contract) when needed
- 24x7x365 device and circuit monitoring to include real-time polling of devices
- Detection, isolation, diagnosis of each fault and restoration to normal operating conditions
- Testing and documenting each fault within the NOC ticketing system
- Ownership of resolution of the problem on behalf of the Clients
- Act as an agent for the Client under executed letters of agency
- Expert User(s) notification of the progress of all faults per the Client provided contact(s) and escalation process
- Safeguard Client's proprietary information
- Take all necessary precautions to ensure a secure connection from the NOC into the Clients network
- Secure Expert User(s) web portal access to
    - View the fault management alarms and event logs
    - Open tickets
    - View contact information

Fault Monitoring

- For each managed device, NOC will monitor up to 10 critical interfaces as identified by the Client during on-boarding. Additional interfaces can be added for an additional fee
- Event Log Montioring - If a critical event occurs the NOC monitoring tools sends out an alert and the NOC will notify the Expert User(s) of the alarm

- Trap Monitoring - The NOC can configure the traps to send critical event information to the network monitoring tools that can create alarms to trigger a trouble ticket
- Problem Identification and Triage - The NOC will notify the Expert User(s). The Service will document the NOC and Expert User(s) acitvities to remediate the isseu and report when the issue has been corrected

Fault Management

- Fault - A fault is defined as a failed device poll indicating the target device is not visible to the NOC network management systems and tools
- If a critical task or function turns off, the NOC will open a ticket and troubleshoot the alarm and resolve the issue. When a fault is identified, the NOC will take ownership of the issue until it is resolved
- The NOC will open a ticket and troubleshoot the cause of alarms. When the cause of the alarm is confirmed, the NOC will resolve the issue
- If the NOC cannot fix the issue directly, the NOC will open a ticket with the vendor (under a vendor maintenance support contract) and work with the vendor support team to resolve the issue, taking ownership until the issue is resolved
- The NOC can configure the traps to send event information to the network monitoring tools, which can trigger a trouble ticket

Configuration Management

- This service provides Access Control giving NOC secure and quick remote access to the managed equipment and keeps an audit trail of who has logged into the client system and when logins occur
- RMS Equipment Configuration Management responsibilities
    - Maintain a log of network device configuration changes
    - Daily polling of each contracted network device to determine if configuration changes have occurred
    - Tracking and archiving of configuration
    - Capturing and archiving the most recent 30 device configuration changes
    - Rapid recovery in the event of configuration loss or changes, or performance issues

Performance and Patch Management

- The NOC monitoring tools measure performance benchmarks of managed network devices to identify and resolve performance bottlenecks in the Client s system
    - The NOC and Expert User(s) must mutually agree on the settings for performance thresholds of all devices
    - The NOC notifies the Expert User(s) when agreed upon device performance thresholds have been exceeded
    - Settings will be evaluated after 90 days of recorded remote monitoring
- Patch Management - The NOC will provide Remote Critical Patch Updates for managed CPE systems
- The NOC will Inform the Expert User(s) about:
    - Critical updates and their availability
    - Current configuration and operational status of the Client devices affected
    - Potential issues with the updates
    - Hardware requirements that for implementing upgrades
- The NOC will perform the remote patch update installation via remote access in accordance with the Client s management processes
- NOC Service includes patch management of 1 patch per quarter, per device or a total of 4 per year. Additional patch management can be supported with professional service hours
- The NOC will periodically review the managed environment and benchmark the environment s performance against NOC optimization standards
- If the NOC recommends any performance improvements, Expert User(s) will be notified in the periodic business review

Device Vendor Management

- The NOC will manage vendors (thru letters of agency) for:
- Replacement parts dispatch thru manufacturer maintenance contracts
- Replacement parts dispatch thru manufacturer maintenance contracts with on-site technician parts replacement
- Incident management with Telco's WAN

- Vendor tickets

Remote Technical Support

- The NOC will work with the hardware vendor (thru letter of authorization) on the Clients behalf to expedite replacement of defective parts. All managed devices are required to have a vendor maintenance contract to provide replacement parts
- The NOC will receive calls from the Expert User(s) or internal IT group after a problem has been identified
- Once a problem has been identified, the NOC will attempt to resolve the issue remotely (i.e., working with Client as needed). If the issue is hardware related, the NOC will open a trouble ticket with the appropriate hardware vendor (under an executed Letter of Agency) and work the problem through resolution

On-site Maintenance

- If on-site device replacement is required, a vendor maintenance contract (with on-site replacement) will need to be purchased by the Client
    - In lieu of an on-site engineer supplied by the NOC, arrangements will have to be made to supply the NOC with an Expert User(s) to provide physical support on-site as directed by the NOC

Support Severity Level Summary

Fault ID	Objective Description	Service Level Response
S1	Detection of Severity 1 (S1) events on the Client network	Within 15 Minutes
S2	Detection of Severity 2 (S2) events on the Client network	Within 15 Minutes
S3	Detection of Severity 3 (S3) events on the Client network	Within 1 hour
S4	Detection of Severity 4 (S4) events on the Client network	Within 2 Business Days

Support Level Definition

(S1) - Critical Severity:

- Produces an emergency in which the network is inoperable, produces incorrect results, or fails catastrophically, or a mainline function of the network is inoperative (i.e., a critical application server), causing significant impact on the Clients business operations (i.e., the Clients production network is down causing critical impact to business operations if service is not restored quickly)
- The NOC and the Client are willing to commit full-time resources around the clock to resolve the situation

(S2) - High Severity:

- Produces a situation in which the network is inoperable, produces incorrect results, or a mainline function of the network is inoperative (i.e., a critical application server), causing a major impact on the Clients business operations (i.e., the Clients production network is severely degraded, impacting significant aspects of business operations)
- The NOC and the Client are willing to commit full-time resources during business hours to resolve the situation

(S3) - Medium Severity:

- Produces a non-critical situation in which the network produces incorrect results, or a feature of the network is inoperative, causing a minor impact on the Client business operations (i.e., the Clients network performance is degraded; network functionality is noticeably impaired, but most business operations continue)
- The NOC shall make commercially reasonable efforts to resolve the problem or provide a workaround as agreed upon between the parties

(S4) - Low Severity:

- General questions, MACD requests and/or inquiries causing little or no impact on the Clients business operations
- The remote management services make commercially reasonable efforts to resolve the problem or provide a workaround as agreed upon between the parties

Device Count Reconciliation

- NOC will conduct a regular audit of total device counts

- Inventory will be compared to the original contract of managed devices to determine if any additions or deletions to the original device count have occurred
- If the number of devices (access point, controller, switches, router, server, etc.) exceed the original contract, the monthly fee will be adjusted
- NOC will onboard all new devices found during the audit and will monitor devices until they are in stable condition and ready for support prior to taking over management
- If issues are discovered during the 2-week period after onboarding a device, NOC will report to the Client/installer to agree on remediation efforts prior to monitoring support beginning. These remediation efforts will be deemed as outside of normal RMS responsibilities and thus will consume professional services hours
- If a device is not able to be successfully on-boarded due to issues, the Client will not be charged the on-boarding fee and the device will be removed from the NOC monitoring systems

Device(s) added after the initial on-boarding will incur a $50 setup fee for each device to cover administrative costs of adding devices to systems and testing connectivity.

Reports

- NOC will provide reports for Expert User(s) about the state of the managed CPE and Applications
- Weekly Reports - These reports look at summarizing the weekly ticket activity showing all tickeets opened, closed and still active tickets
- Monthly Reports - These monthly reports look at the contracted infrastructure devices. The reports include statistics on:
    - Network, device uptime and availability
    - Fault history
    - Trouble tickets
    - Professional Services hours used

Strategic Reporting

- Periodic Business Review - Provides business intelligence information based on the data that the NOC gathers during the period under review. This information has potential business impacting information that reflects
- CPE network trends observed
- Capacity planning
- Resource utilization trends
- Ticketing trends
- Compliance issues
- Normal operating specifications
- Security concerns and business continuity planning
- The goal of this report is to:
    - Characterize the existing managed environment
    - Make specific recommendations for improvement
    - Trouble tickets
    - Provide budgetary information to implement the recommendations

Report-based recommendations

- Immediate Impact recommendations provide an immediate impact on performance across the managed network
- High Impact recommendations provide additional improvements in performance as well as increasing network management efficiency
- Strategic recommendations focus on ensuring that the network will scale to meet future business requirements and that the Client will be able to proactively monitor and manage network performance using the NOC
- Performance Analysis - Provides information about the overall performance of the managed network showing
    - Bottlenecks
    - Areas of high utilization
    - Areas of under-utilization
    - Dropped packets

Unusually high error rates
- Lower than normal device uptime

Report-based recommendations

- Triage of network device incidents
- Troubleshoot and work to resolve network device incidents
- Document network device errors

Move, Add, Change, Deletes (MACD)

- MACD is provided under a separate ItemID. See ItemID 604367.

Professional Services Block of Hours

- A Professional Services Block of Hours is provided under a separate ItemID. See ItemID 604366.

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

- Those defined as Expert Users will be forward to NDS as Customer Designated Contacts

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Client must have contracted for MACD and Professional Services
- Only Expert User(s) should call the NOC directly to ask questions regarding use of the servers, applications, features or capabilities
- All managed devices are required to have a vendor maintenance contract to provide replacement parts

Out of Scope Activities

- Staging, configuring, and installing equipment for non- break fix related issues
- System re-configuration to support product replacement of CPE or for non-break fix issues (Examples may include, but are not limited to, replacing devices due to end of life or end of support or replacement of devices for convenience.) These requests can be supported with extend support hours or as a separate project
- Major re-configuration activities to support non-break fix activities (not including MACD)
- Creation of custom reporting
- General help desk support for users not defined as Expert Users
- Updating of Client workstations or mobile devices to meet policy-based requirements
- Creation of firewall configuration and security policies
- Supporting Client PC, laptops, or mobile devices for non-connectivity issues (including, but not limited to, device application issues or device OS/IOS issues)
- Supporting third party applications that are not defined as part of the NOC
- Monitoring and management of Client CPE (routers, switches, or other devices) not defined in the Service Initiation Form
- Onsite NOC support, unless Onsite Remote Managed (OMS) service option is selected
- Client access to conductor or orchestration service platform
- NOC assumes no liability for security breaches, security policies, denial of service incidents, or other related security

incidents
- Remediation of production issues on the current infrastructure
- Optimization or re-configuration activities for current infrastructure
- Equipment staging services for solution devices and equipment
- Network and firewall configuration support for current infrastructure to enable services
- Troubleshooting Client applications traversing service
- On-site support for equipment installation and project services
- Assessment or site survey services to conduct discovery of Client s current network and application environment
- Decommissioning and removal of any existing customer owned equipment in not within the scope of this engagement

604364 Network Data Systems Managed Aruba Access Point

Company's Responsibilities and Included Features

Remote Managed Service (RMS) for Client Premise Equipment (CPE) is provided by Network Data Systems, Inc. (NDS) through the NDS Network Operation Center (NOC) in accordance with the Network Data Systems Addendum to the Statement of Work. This SKU provides for the hardware management of Aruba access points through the NDS NOC RMS.

Remote Managed NOC Services (RMS)

- In the event there is a site related issue (loss of power to site, damage to premise cabling, accidental disconnection of cabling or equipment, or carrier issues) that causes an outage of devices or systems under management, the NOC will document the issue within the NOC ticketing system, notify the Expert User(s), and manage the issue until resolution. The NOC will close the ticket once the site related issue is remediated. When the ticket is closed, the Clients designated contact will receive an email indicating that the site issue is resolved
- If a contracted device has a component hardware failure, the NOC will diagnose and attempt to resolve the issue remotely. If the hardware failure cannot be resolved remotely, the NOC will begin dispatch of a replacement part (via the Clients vendor maintenance support contract) when needed
- 24x7x365 device and circuit monitoring to include real-time polling of devices
- Detection, isolation, diagnosis of each fault and restoration to normal operating conditions
- Testing and documenting each fault within the NOC ticketing system
- Ownership of resolution of the problem on behalf of the Clients
- Act as an agent for the Client under executed letters of agency
- Expert User(s) notification of the progress of all faults per the Client provided contact(s) and escalation process
- Safeguard Client's proprietary information
- Take all necessary precautions to ensure a secure connection from the NOC into the Clients network
- Secure Expert User(s) web portal access to
    - View the fault management alarms and event logs
    - Open tickets
    - View contact information

Fault Monitoring

- For each managed device, NOC will monitor up to 10 critical interfaces as identified by the Client during on-boarding. Additional interfaces can be added for an additional fee
- Event Log Montioring - If a critical event occurs the NOC monitoring tools sends out an alert and the NOC will notify the Expert User(s) of the alarm
- Trap Monitoring - The NOC can configure the traps to send critical event information to the network monitoring tools that can create alarms to trigger a trouble ticket
- Problem Identification and Triage - The NOC will notify the Expert User(s). The Service will document the NOC and Expert User(s) acitvities to remediate the isseu and report when the issue has been corrected

Fault Management

- Fault - A fault is defined as a failed device poll indicating the target device is not visible to the NOC network management systems and tools

If a critical task or function turns off, the NOC will open a ticket and troubleshoot the alarm and resolve the issue. When a fault is identified, the NOC will take ownership of the issue until it is resolved

- The NOC will open a ticket and troubleshoot the cause of alarms. When the cause of the alarm is confirmed, the NOC will resolve the issue
- If the NOC cannot fix the issue directly, the NOC will open a ticket with the vendor (under a vendor maintenance support contract) and work with the vendor support team to resolve the issue, taking ownership until the issue is resolved
- The NOC can configure the traps to send event information to the network monitoring tools, which can trigger a trouble ticket

Configuration Management

- This service provides Access Control giving NOC secure and quick remote access to the managed equipment and keeps an audit trail of who has logged into the client system and when logins occur
- RMS Equipment Configuration Management responsibilities
    - Maintain a log of network device configuration changes
    - Daily polling of each contracted network device to determine if configuration changes have occurred
    - Tracking and archiving of configuration
    - Capturing and archiving the most recent 30 device configuration changes
    - Rapid recovery in the event of configuration loss or changes, or performance issues

Performance and Patch Management

- The NOC monitoring tools measure performance benchmarks of managed network devices to identify and resolve performance bottlenecks in the Client s system
    - The NOC and Expert User(s) must mutually agree on the settings for performance thresholds of all devices
    - The NOC notifies the Expert User(s) when agreed upon device performance thresholds have been exceeded
    - Settings will be evaluated after 90 days of recorded remote monitoring
- Patch Management - The NOC will provide Remote Critical Patch Updates for managed CPE systems
- The NOC will Inform the Expert User(s) about:
    - Critical updates and their availability
    - Current configuration and operational status of the Client devices affected
    - Potential issues with the updates
    - Hardware requirements that for implementing upgrades
- The NOC will perform the remote patch update installation via remote access in accordance with the Client s management processes
- NOC Service includes patch management of 1 patch per quarter, per device or a total of 4 per year. Additional patch management can be supported with professional service hours
- The NOC will periodically review the managed environment and benchmark the environment s performance against NOC optimization standards
- If the NOC recommends any performance improvements, Expert User(s) will be notified in the periodic business review

Device Vendor Management

- The NOC will manage vendors (thru letters of agency) for:
- Replacement parts dispatch thru manufacturer maintenance contracts
- Replacement parts dispatch thru manufacturer maintenance contracts with on-site technician parts replacement
- Incident management with Telco's WAN
- Vendor tickets

Remote Technical Support

- The NOC will work with the hardware vendor (thru letter of authorization) on the Clients behalf to expedite replacement of defective parts. All managed devices are required to have a vendor maintenance contract to provide replacement parts
- The NOC will receive calls from the Expert User(s) or internal IT group after a problem has been identified
- Once a problem has been identified, the NOC will attempt to resolve the issue remotely (i.e., working with Client as

needed). If the issue is hardware related, the NOC will open a trouble ticket with the appropriate hardware vendor (under an executed Letter of Agency) and work the problem through resolution

On-site Maintenance

- If on-site device replacement is required, a vendor maintenance contract (with on-site replacement) will need to be purchased by the Client
    - In lieu of an on-site engineer supplied by the NOC, arrangements will have to be made to supply the NOC with an Expert User(s) to provide physical support on-site as directed by the NOC

Support Severity Level Summary

Fault ID	Objective Description	Service Level Response
S1	Detection of Severity 1 (S1) events on the Client network	Within 15 Minutes
S2	Detection of Severity 2 (S2) events on the Client network	Within 15 Minutes
S3	Detection of Severity 3 (S3) events on the Client network	Within 1 hour
S4	Detection of Severity 4 (S4) events on the Client network	Within 2 Business Days

Support Level Definition

(S1) - Critical Severity:

- Produces an emergency in which the network is inoperable, produces incorrect results, or fails catastrophically, or a mainline function of the network is inoperative (i.e., a critical application server), causing significant impact on the Clients business operations (i.e., the Clients production network is down causing critical impact to business operations if service is not restored quickly)
- The NOC and the Client are willing to commit full-time resources around the clock to resolve the situation

(S2) - High Severity:

- Produces a situation in which the network is inoperable, produces incorrect results, or a mainline function of the network is inoperative (i.e., a critical application server), causing a major impact on the Clients business operations (i.e., the Clients production network is severely degraded, impacting significant aspects of business operations)
- The NOC and the Client are willing to commit full-time resources during business hours to resolve the situation

(S3) - Medium Severity:

- Produces a non-critical situation in which the network produces incorrect results, or a feature of the network is inoperative, causing a minor impact on the Client business operations (i.e., the Clients network performance is degraded; network functionality is noticeably impaired, but most business operations continue)
- The NOC shall make commercially reasonable efforts to resolve the problem or provide a workaround as agreed upon between the parties

(S4) - Low Severity:

- General questions, MACD requests and/or inquiries causing little or no impact on the Clients business operations
- The remote management services make commercially reasonable efforts to resolve the problem or provide a workaround as agreed upon between the parties

Device Count Reconciliation

- NOC will conduct a regular audit of total device counts
- Inventory will be compared to the original contract of managed devices to determine if any additions or deletions to the original device count have occurred
- If the number of devices (access point, controller, switches, router, server, etc.) exceed the original contract, the monthly fee will be adjusted
- NOC will onboard all new devices found during the audit and will monitor devices until they are in stable condition and ready for support prior to taking over management
- If issues are discovered during the 2-week period after onboarding a device, NOC will report to the Client/installer to agree on remediation efforts prior to monitoring support beginning. These remediation efforts will be deemed as

outside of normal RMS responsibilities and thus will consume professional services hours
- If a device is not able to be successfully on-boarded due to issues, the Client will not be charged the on-boarding fee and the device will be removed from the NOC monitoring systems

Device(s) added after the initial on-boarding will incur a $50 setup fee for each device to cover administrative costs of adding devices to systems and testing connectivity.

Reports

- NOC will provide reports for Expert User(s) about the state of the managed CPE and Applications
- Weekly Reports - These reports look at summarizing the weekly ticket activity showing all tickeets opened, closed and still active tickets
- Monthly Reports - These monthly reports look at the contracted infrastructure devices. The reports include statistics on:
    - Network, device uptime and availability
    - Fault history
    - Trouble tickets
    - Professional Services hours used

Strategic Reporting

- Periodic Business Review - Provides business intelligence information based on the data that the NOC gathers during the period under review. This information has potential business impacting information that reflects
- CPE network trends observed
- Capacity planning
- Resource utilization trends
- Ticketing trends
- Compliance issues
- Normal operating specifications
- Security concerns and business continuity planning
- The goal of this report is to:
    - Characterize the existing managed environment
    - Make specific recommendations for improvement
    - Trouble tickets
    - Provide budgetary information to implement the recommendations

Report-based recommendations

- Immediate Impact recommendations provide an immediate impact on performance across the managed network
- High Impact recommendations provide additional improvements in performance as well as increasing network management efficiency
- Strategic recommendations focus on ensuring that the network will scale to meet future business requirements and that the Client will be able to proactively monitor and manage network performance using the NOC
- Performance Analysis - Provides information about the overall performance of the managed network showing
    - Bottlenecks
    - Areas of high utilization
    - Areas of under-utilization
    - Dropped packets
    - Unusually high error rates
    - Lower than normal device uptime

Report-based recommendations

- Triage of network device incidents
- Troubleshoot and work to resolve network device incidents
- Document network device errors

Move, Add, Change, Deletes (MACD)

- MACD is provided under a separate ItemID. See ItemID 604367.

Professional Services Block of Hours

- A Professional Services Block of Hours is provided under a separate ItemID. See ItemID 604366.

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

- Those defined as Expert Users will be forward to NDS as Customer Designated Contacts

Client's Responsibilities and Out-of-Scope Notes (unless covered by another ItemID)

- Client must have contracted for MACD and Professional Services
- Only Expert User(s) should call the NOC directly to ask questions regarding use of the servers, applications, features or capabilities
- All managed devices are required to have a vendor maintenance contract to provide replacement parts

Out of Scope Activities

- Staging, configuring, and installing equipment for non- break fix related issues
- System re-configuration to support product replacement of CPE or for non-break fix issues (Examples may include, but are not limited to, replacing devices due to end of life or end of support or replacement of devices for convenience.) These requests can be supported with extend support hours or as a separate project
- Major re-configuration activities to support non-break fix activities (not including MACD)
- Creation of custom reporting
- General help desk support for users not defined as Expert Users
- Updating of Client workstations or mobile devices to meet policy-based requirements
- Creation of firewall configuration and security policies
- Supporting Client PC, laptops, or mobile devices for non-connectivity issues (including, but not limited to, device application issues or device OS/IOS issues)
- Supporting third party applications that are not defined as part of the NOC
- Monitoring and management of Client CPE (routers, switches, or other devices) not defined in the Service Initiation Form
- Onsite NOC support, unless Onsite Remote Managed (OMS) service option is selected
- Client access to conductor or orchestration service platform
- NOC assumes no liability for security breaches, security policies, denial of service incidents, or other related security incidents
- Remediation of production issues on the current infrastructure
- Optimization or re-configuration activities for current infrastructure
- Equipment staging services for solution devices and equipment
- Network and firewall configuration support for current infrastructure to enable services
- Troubleshooting Client applications traversing service
- On-site support for equipment installation and project services
- Assessment or site survey services to conduct discovery of Client s current network and application environment
- Decommissioning and removal of any existing customer owned equipment in not within the scope of this engagement

604365 Network Data Systems Managed Device Onboarding

Company's Responsibilities and Included Features

Remote Managed NOC Service (RMS) for Client Premise Equipment (CPE) is provided by Network & Data Systems (NDS) through the NDS Network Operation Center (NOC) in accordance with the Network Data Systems Addendum to the Statement of Work. This Item ID provides for the onboarding of devices to be covered under the RMS.

Remote Managed NOC Services (RMS) Onboarding

- NOC team will escalate to vendor using the on-site vendor maintenance contract for hardware parts replacement on all devices under support
- NOC will use standard operational procedures for connectivity and access to Client environment. Custom connectivity and access procedures will be evaluated and supported via Change Orders, as required
- NOC will not take responsibility for remote management of any existing devices or systems until the existing system is validated to be functioning properly
- NOC will issue a charge order for remediation support if the system is not functioning properly and the Client requests help from the NOC
- In the case the Client is experiencing performance issues, the NOC will check the devices under management to determine if they are within expected operating thresholds. If the devices are within expected thresholds, the NOC will alert the Client that all contracted devices are performing as expected and that the cause of the problem is outside of the managed devices

Out of Scope Activities

- Staging, configuring, and installing equipment for non- break fix related issues
- System re-configuration to support product replacement of Client premise equipment or for non-break fix issues. (Example, to include but not limited to, replacing devices due to end of life or end of support or replacement of devices for convenience.) These requests can be supported with extend support hours or as a separate project
- Major re-configuration activities to support non-break fix activities. (Not including MACD)
- Creation of Custom Reporting
- General help desk support for users not defined as Expert Users
- Updating of Client workstations or mobile devices to meet policy-based requirements
- Creation of Firewall configuration and security policies
- Supporting Client PC, laptops, or mobile devices for non-connectivity issues to include but not limited to device application issues or device OS/IOS issues
- Supporting third party applications that are not defined as part of the NOC
- Monitoring and management of client CPE (routers, switches, or other devices) not defined in the Service Initiation Form
- Onsite NOC support, unless Onsite Remote Managed (OMS) service option is selected
- Client access to conductor or orchestration service platform
- NOC assumes no liability for security breaches, security policies, denial of service incidents, or other related security incidents

Network Device Triage and Troubleshooting

- Triage of network device incidents
- Troubleshoot and work to resolve network device incidents
- Document network device errors

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the

An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

- Those defined as Expert Users will be forwarded to NDS as Customer Designated Contacts

Client s Responsibilities and Out-of-Scope Notes

Clients are responsible for completing the below duties before the RMS begins.

- Complete Service Initiation Form
  - Provide all contracted CPE and Application information to enable the NOC to discover the contracted devices
  - Load site information into the NOC systems per a correctly and fully completed Service Initiation Form that includes, but is not limited to:
    - Device information
    - System access
    - Network diagrams
    - Site information
    - Client contact information
    - Circuit information
    - Client HW/SW vendor maintenance contracts
    - Letters of Agency to vendors
    - Current software levels and patch levels
- Provide network diagrams
- Provide as-built documentation
- Provide configuration files
- Provide security profiles or other applicable documentation regarding supported devices
- Have a valid vendor maintenance contract for all contracted devices and applications under managed services
- Provide access to vendor maintenance contracts
- Have a valid on-site vendor maintenance contract for hardware parts replacement on all devices under support, enabling on site hardware replacement when required
- Provide the NOC connectivity to all contracted CPE devices under the support service contract
- Provide the NOC with the following security information including (but not limited to)
  - Dial-in numbers
  - Access ID's
  - Passwords
  - SNMP community names necessary for the NOC to perform the contracted support services. Note: Any device under the support services contract should be SNMP capable
- Take on financial responsibility for any required WAN/ISP circuits to support the NOC solution
- Provide proper bandwidth requirements for their WAN and ISP transport services
- Provide list of Expert User(s)
- Responsible for monitoring, managing, troubleshooting, configuration changes and break fix support for these devices and circuits connected to these devices CPE (routers, switches, or other devices) not defined in the Service Initiation Form . Service Level Objective calculations will not include client monitored and managed devices

Minimum Standards Remote Managed Service

NOC is based on standards and minimums outlined below. If these standards and minimums are not maintained, NOC pricing will be impacted.

- CPE devices and applications supported by NOC must be no more than 2 revisions from the latest major release from the vendor. These versions must also still be supported by the vendor and the Client must have an active maintenance service contract in place for each contracted device
- Devices under NOC contract must be configured to adhere to NOC-defined best practices to ensure stability and security. This includes but is not limited to:

        - Passwords encrypted and complex
        - Using SSH vs. Telnet
        - Not openly accessible via internet
        - NTP configured and pointing towards reliable server
        - Ensure failover is configured and working properly when redundancy is in place
        - Backups are configured and working properly and periodically tested and validated at least once per year
        - Redundancy is configured and working. Failover should be tested at least once a year. Client to provide evidence of last test and results/actions
    - Devices under NOC contract must be properly implemented and functioning as designed in the production environment prior to NOC beginning
    - Client is responsible for alerting the NOC of changes to their network that could affect their devices under the support services contract
    - Client is responsible for alerting the NOC of any security requirements for monitoring of infrastructure
    - In the case that the system is not functioning properly, the Client can have NOC remediate any issues to a steady state condition or the Client can remediate the issues themselves
    - Time and Material billing for re-installation of equipment or operating systems improperly installed by someone other than the NOC or problems caused by Client or other vendors accessing the network
    - Client must provide the NOC with legal copies and licenses for all software and applications that are under monitoring and management
    - The Client s IT team will have the responsibility to identify and resolve the issue if the Client is experiencing performance issues while the devices under management are within expected operating thresholds
    - Devices must always be powered on. If recurring issues are identified that are not able to be resolved by the NOC due to the environment, NOC will provide 30 days notification and discontinue proactive monitoring
    - Client must be able to provide documentation of a site to aid in troubleshooting physical and environmental issues. If this cannot be provided, NOC will not be able to proactively monitor and in some cases manage devices. If necessary, the device vendor will provide a statement of work to identify and make recommendations for remediation of physical or environmental issues
    - In the event e-bonding is required for this service NOC will work in good faith with the Client to establish e-bonding requirements in a reasonable, agreed to timeframe. E-bonding service will be delivered under a Change Order (CO) defining scope and additional costs outside of the current statement of work
    - NOC Service are English based for all communications. Multi-language services are out of scope

604366 Network Data Systems Professional Services Hours (per Year)

Company's Responsibilities and Included Features

Remote Managed NOC Service (RMS) for Client Premise Equipment (CPE) is provided by Network & Data Systems (NDS) through the NDS Network Operation Center (NOC) in accordance with the Network Data Systems Addendum to the Statement of Work. This Item ID provides for the professional service hours used by the NOC to perform operations outside of normal RMS responsibilities for managed devices.

RMS for switches, routers, or wireless access points (item IDs 604362, 604363, or 604364) are a prerequisite for this Item ID.

Professional Services

- The NOC includes professional service hours for RMS devices for Expert User(s) requests beyond normal device problem management included in the scope of the Statement of Work (SOW) or responses to questions regarding covered devices
- The NOC will perform the requested support and track the hours utilized and report on the usage and hours remaining in the monthly report
- The professional services hours will be provided via remote support and will be used for non-break fix support or small project-based activities
- Large projects requiring additional time, beyond the allotment of professional service hours, will be provided in a separate SOW and will be delivered as a project outside of this managed support agreement
- Upon request for custom reports, they will be available with the use of professional service hours

Network Device Triage and Troubleshooting

- Triage of network device incidents
- Troubleshoot and work to resolve network device incidents
- Document network device errors

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

- Those defined as Expert Users will be forwarded to NDS as Customer Designated Contacts

Client s Responsibilities and Out-of-Scope Notes

604367 Network Data Systems MACD (per Year)

Company's Responsibilities and Included Features

Remote Managed NOC Service (RMS) for Client Premise Equipment (CPE) is provided by Network & Data Systems (NDS) through the NDS Network Operation Center (NOC) in accordance with the Network Data Systems Addendum to the Statement of Work. This Item ID provides for move, add, change, delete (MACD) requests from the Client to the NOC.

RMS for switches, routers, or wireless access points (item IDs 604362, 604363, or 604364) are a prerequisite for this Item ID.

MACD (Moves, Adds, Changes & Deletions)

- Device Administration - The NOC will remotely add and remove devices from your system, reset passwords, and assign new passwords
- This provides MACDs for RMS devices
- Up to 50 MACD can be submitted every 48 hours. In the event the Client requires more than 50 MACDs within 48 hours, the MACDs exceeding 50 will be completed under a revised service level objective of 5 business days for targeted completion
- The MACDs will be performed remotely by the NOC. The NOC will complete requested MACDs within 48 hours of receipt of the remote MACD request
- Remote MACDs will be handled Monday-Friday 8 a.m. to 8 p.m. EST
- Monthly reports will provide statistics on MACDs used

WEB Portal Access

The NOC can provides access into the ticketing system and monitoring tools via a secure WEB portal. The WEB portal is configured provide 24x7x365 read only access into the Clients devices and tickets. The WEB portal can provide the following to the Expert User(s):

A list of Expert User(s) will need to be provided to the NOC by the Client for access into the WEB portal via the Service Initiation Form. WEB portal training (1 hour) for the Expert User(s) portal uses will be scheduled thru the NOC.

- View open and closed tickets
- Open a new S3 or S4 ticket
- Expert User(s) contact information
- View Client (CPE) devices in real time using the NOC monitoring tools

- Device and Application Performance Information
    - Device CPU utilization
    - Device memory utilization
    - Storage utilization
    - Power supplies
    - Fans
    - Temperature

Network Device Triage and Troubleshooting

- Triage of network device incidents
- Troubleshoot and work to resolve network device incidents
- Document network device errors

Expert User Technical Support

Technical support may only be requested by a Client Expert User*, available during the following hours:

- 24 x 7 technical support for priority 1 and 2 incidents
- 6 am to 5 pm MST, Monday to Friday technical support for priority 3, 4 and 5 incidents
- Priority is determined by Company based on the combination of impact and urgency to Client as further provided in the OneNeck Customer Operations Handbook

An Expert User is defined as someone with in-depth application or system knowledge and is authorized by Client to request support or changes be made to the configuration of the system. The number of Expert Users is limited to 5 or 5% of the Client staff, whichever is greater.

- Those defined as Expert Users will be forwarded to NDS as Customer Designated Contacts

Client s Responsibilities and Out-of-Scope Notes