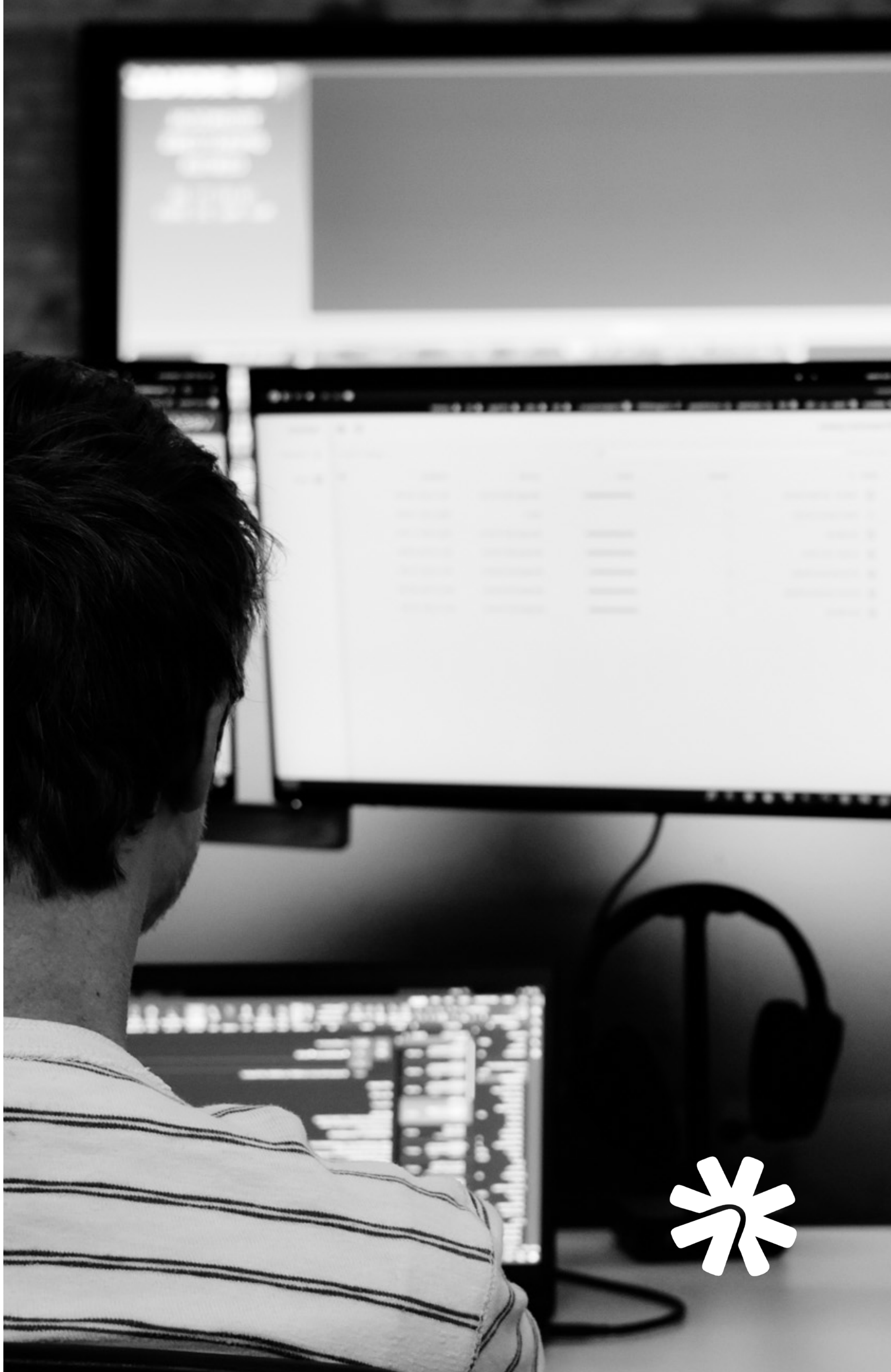
Implementing DRaaS in Your IT Environment: A Guide to Getting Started

us signal

Table of Contents



Introduction

Data is the lifeblood of your business, driving decision-making, enabling customer interactions, and supporting daily operations. However, as data becomes increasingly central to business functions, it becomes more vulnerable. Unplanned incidents such as natural disasters, cyberattacks, human errors, and hardware failures can lead to significant data loss and operational disruptions.

Recovering quickly from these disasters requires a well-thought-out disaster recovery (DR) plan. A robust DR plan outlines the procedures and resources needed to restore data and resume critical business functions after a disruption. However, developing and maintaining such a plan can be costly and resource-intensive, often requiring significant investment in infrastructure and dedicated personnel.

Disaster Recovery as a Service (DRaaS) offers an ideal solution for many small- to mid-sized businesses. DRaaS provides a cloud-based approach to disaster recovery, allowing companies to leverage advanced technologies and expert management without traditional DR methods' high costs and complexity.

Creating Your DR Strategy

- **Assess Your Business Goals:** Evaluate the key objectives your disaster recovery plan must achieve.
- **Identify Current Limitations:** Understand the limitations and constraints within your existing IT environment.
- **Determine RTO:** Establish your Recovery Time Objective, which is the maximum acceptable time to restore services.
- **Determine RPO:** Set your Recovery Point Objective, which is the maximum acceptable amount of data loss measured in time.
- **Create a DR Plan/Playbook:** Develop a comprehensive disaster recovery plan that outlines procedures and protocols.
- **Define Roles/Responsibilities:** Assign specific roles and responsibilities for disaster recovery within your team.

Creating a DR Plan

Create a detailed DR plan that outlines the steps and sequence of recovery actions:

Design the Target DR Site: Configure the target DR site to match your production environment as closely as possible.

Develop Custom Scripts: If necessary, create custom scripts to automate recovery processes.

Align with Existing Procedures: Ensure the new DRaaS works seamlessly with your recovery procedures.

Assemble DR Team: Form a team with clear recovery roles and responsibilities.

Initial and Ongoing Testing

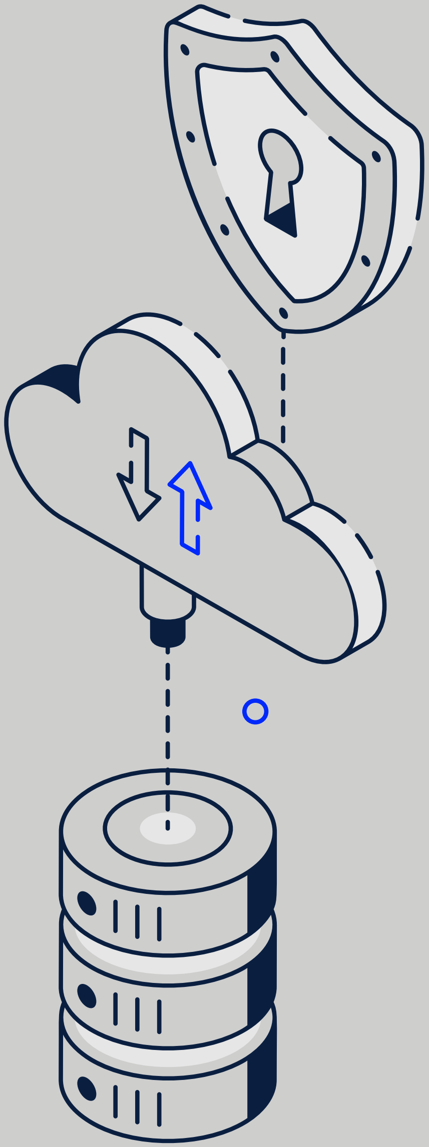
Testing is essential to validate the effectiveness of your DR plan:

Select Snapshots and Validate Failover: Choose specific snapshots and perform failover tests to ensure systems can be recovered as planned.

Update and Retest: If any issues are found during testing, update
the DR plan until it is reliable and consistent.

Test Regularly: Schedule regular tests to validate the DR plan's effectiveness.

Document and Implement Changes: Integrate any changes into your existing procedures.



Preparing & Setting Up Your IT Environment

01

Conduct a Comprehensive Inventory

Inventory All Assets: Document all hardware, software, applications, and data within your IT environment. Include physical servers, virtual machines, network devices, storage systems, and critical applications.

Identify Critical Assets: Determine which assets are crucial to your business operations and prioritize them for disaster recovery.

02

Assess Current IT Infrastructure

Evaluate Infrastructure Health: Check the current state of your IT infrastructure, including server performance, storage capacity, and network bandwidth. Identify any weaknesses or areas that need upgrades to support DRaaS.

Compatibility Check: Ensure your infrastructure components are compatible with the chosen DRaaS solution.

03

Map Application Dependencies

Dependency Mapping: Identify and document the interdependencies between applications and systems. Understanding these dependencies is crucial for effective disaster recovery planning.

Service Level Requirements: Define the service level requirements for each application, including acceptable downtime and data loss,
to align with your recovery objectives.

04

Evaluate Network Requirements

Network Bandwidth Analysis: Assess your network's bandwidth to ensure it can handle the data replication and recovery operations required by the DRaaS solution.

Latency and Throughput: Measure network latency and throughput to identify potential bottlenecks impacting DRaaS performance.

Compliance & Security Obligations

Ensure Compliance with Regulatory Standards

Identify Relevant Regulations: Determine the regulatory requirements applicable to your organization, such as GDPR, HIPAA, or PCI-DSS.

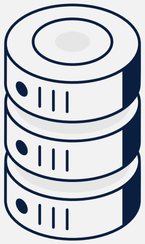
Compliance Assessment: Conduct a compliance assessment to ensure your DRaaS solution meets all regulatory standards. This includes data encryption, access controls, and audit logging.

Implement Security Measures

Data Encryption: Ensure data is encrypted during transmission and storage to protect against unauthorized access.

Access Controls: Implement strict access controls to limit who can access and manage the DRaaS environment. Use multi-factor authentication (MFA) for added security.

Regular Security Audits: Schedule regular security audits to identify and address potential vulnerabilities within your DRaaS setup.



Data Backup & Replication

Initial Data Backup and Continuous Replication

Initial Data Backup: Perform a full backup of all critical data and systems to the DRaaS provider's infrastructure. Depending on the volume of data, this process may take time.

Continuous Data Replication: Set up continuous or scheduled data replication to ensure that any changes to your data are promptly mirrored in the DRaaS environment. This step is vital to minimize data loss in case of a disaster.

Configuring DRaaS Settings

Define Recovery Plans and Objectives

Defining Recovery Plans: Create detailed recovery plans for each critical system and application. These plans should outline the steps during a disaster recovery scenario.

Setting RTO and RPO: Configure each system's Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), ensuring they align with your business requirements.

Testing Failover Processes: Conduct initial tests to ensure that the failover processes work as expected and that data can be recovered within the defined RTO and RPO.

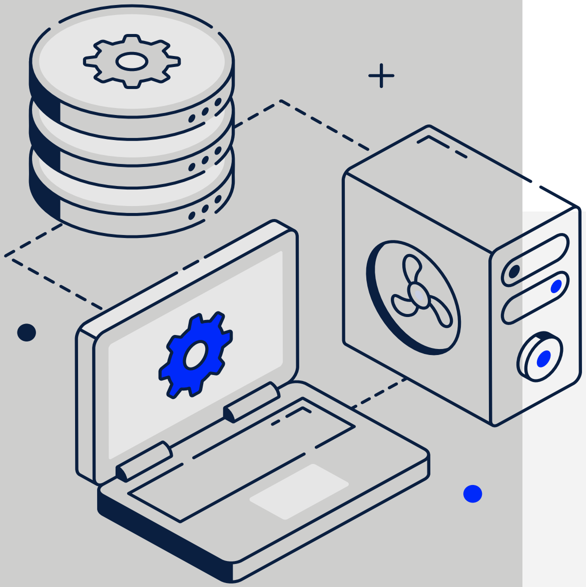
Management & Optimization

Management

Once your DRaaS solution is operational, ongoing monitoring and maintenance are crucial for ensuring its effectiveness:

Real-Time Monitoring: Use monitoring tools provided by your DRaaS provider to track the health and performance of your disaster recovery environment. Monitor for replication lag, storage capacity, and system errors.

Regular Maintenance Tasks: Perform routine maintenance tasks such as updating software, applying patches, and conducting performance tuning to keep your DRaaS solution running smoothly.



Optimizing DRaaS Performance

Consider the following optimization strategies to maximize the effectiveness of your DRaaS solution:

Performance Tuning: Regularly review and optimize the performance of your DRaaS environment. This might involve adjusting replication settings, upgrading network components, or fine-tuning recovery plans.

Leveraging Analytics: Utilize analytics tools to gain insights into your DRaaS operations. Analyze data to identify trends, potential bottlenecks, and areas for improvement. Use these insights to make informed decisions and continuously enhance your disaster recovery strategy.

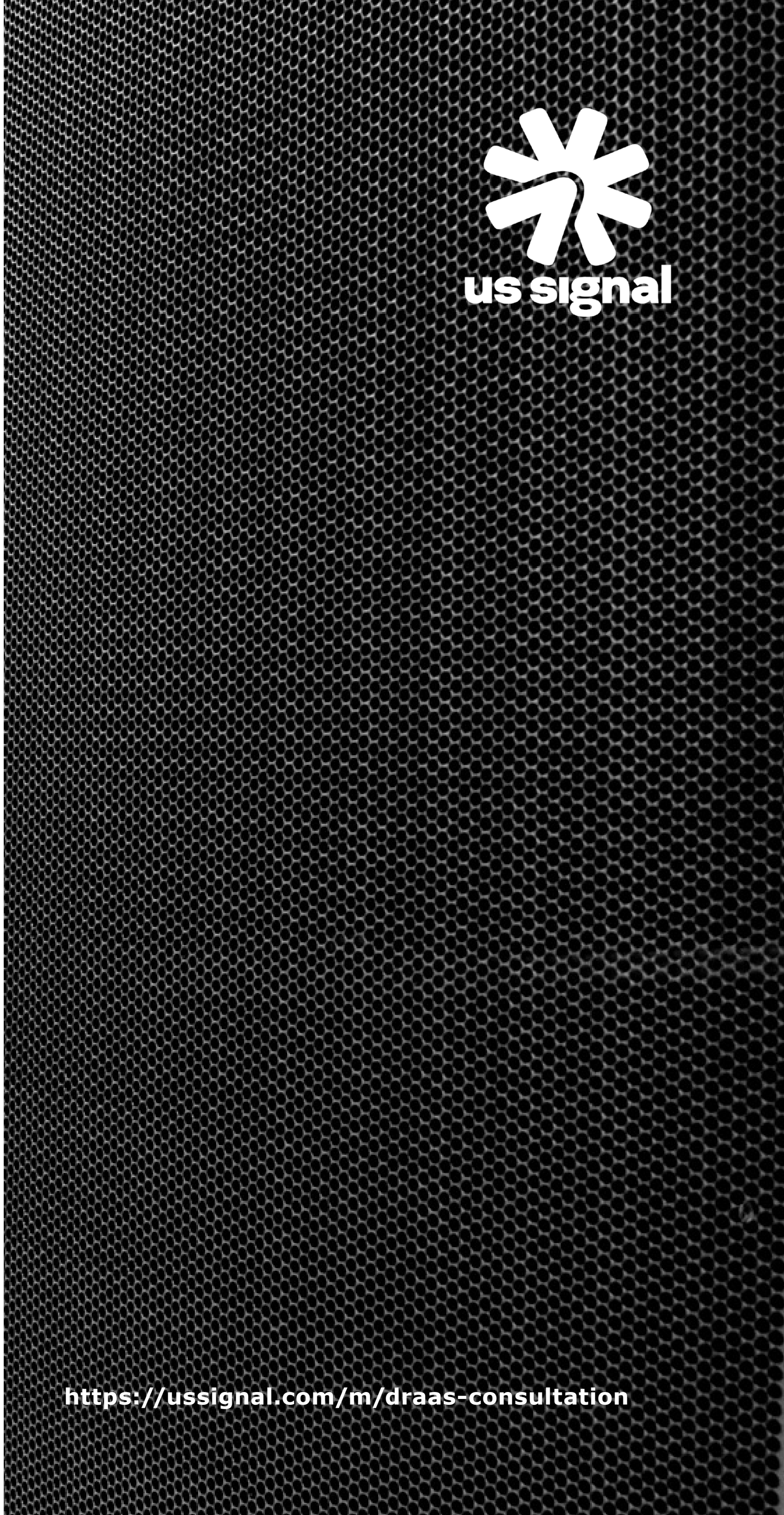
ReliaCloud DRaaS & Managed Services

At US Signal, we work with our clients to carefully assess their data infrastructure and requirements, developing a disaster recovery strategy to meet their needs. Our ReliaCloud® (built on Nutanix™) solution allows you to confidently achieve SLAs with a cloud-based disaster recovery service featuring instant failover, failback, or test recovery plans, all with just a few clicks.

ReliaCloud DRaaS leverages state-of-the-art technology to provide robust disaster recovery capabilities, ensuring rapid recovery and minimal downtime. Our platform scales with your business and includes advanced security measures like encryption, access controls, and regular security audits to safeguard against unauthorized access and breaches, all while ensuring compliance with regulatory standards.

US Signal offers total management and operation of your DRaaS solution, taking the burden off your team. Our managed services include 24/7 support to address any issues, proactive monitoring to track the health and performance of your environment in real time, and regular maintenance to keep your DRaaS solution up-to-date. You can confidently protect your critical systems and data by choosing US Signal's ReliaCloud DRaaS and Managed Services.

ussignal.com | 866.274.4625 | info@ussignal.com



us signal

https://ussignal.com/m/draas-consultation