DISASTER RECOVERY-AS-A-SERVICE

The US Signal Disaster Recovery-as-a-Service is powered by the Zerto Virtual Replication platform to provide you with near continuous block-level replication of critical workloads. Virtual machines are protected from their production data center to a US Signal cloud data center.

At-a-Glance

+ Fully managed data protection offering with near continuous block-level replication providing tested RPOs of seconds and RTOs of minutes
+ Developed and managed DR Playbook encompassing protection and recovery processes and operations
+ Supports both VMware ESX/ESXi and Microsoft Hyper-V source environments
+ Built-in data compression to reduce bandwidth requirements for initial data sync and ongoing replication
+ Managed recovery testing to validate recovery operations with supporting reports to satisfy compliance requirements
+ Recovery of individual applications or entire data centers with the click of a button
+ Granular point-in-time recovery with write-order fidelity across all protected virtual machines in a single virtual protection group

TECHNICAL OVERVIEW

US Signal Managed Services Engineers will work with your team to deploy the required Zerto software components within the source compute environment. Once the software components have been deployed and the private network connectivity is established, the replication of workloads will be configured and monitored by US Signal. The following software components will be installed in your source environment:

ZVM (Zerto Virtual Manager)

Windows-based virtual machine that is used to monitor and manage replication activity, site links, VPGs (Virtual Protection Groups), and protected VMs. The site ZVM is designed to be installed on a dedicated server that has network connectivity to vCenter or SCVMM.

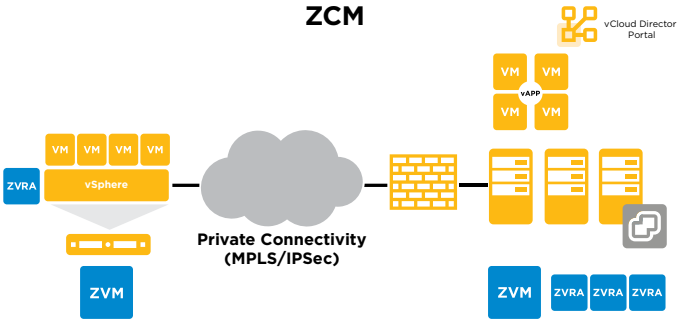
ZCM (Zerto Cloud Manager)

Windows-based service that is used as a management layer above the ZVM. An individual ZVM controls one site, the ZCM manages multiple ZVM's and their respective sites.

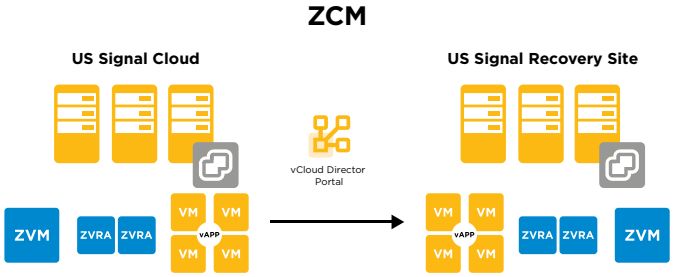
VRA (Virtual Replication Appliance)

Debian Linux-based virtual machine that is installed on each ESXi/Hyper-V host in the environment. The purpose of this appliance is to intercept all I/O (data) writes to a protected VMs storage. The appliance will then clone it, compress it, and write operations to the VRA in the recovery environment which will be written to the recovery volume and the journal.

Disaster Recovery-as-a-Service Tech Sheet



Customer Premises to US Signal Cloud



US Signal Cloud Resiliency

AGENT COMPATIBILITY

As the Zerto Virtual Replication platform works at the hypervisor level, there are no inherent conflicts with other agents that may be operating on the protected virtual machines. Traditional backup software can still be utilized to provide an additional layer of data protection for the workloads.

REPLICATION OPERATIONS AND FEATURES

Every I/O write from a protected virtual machine in the source environment is copied by the VRA appliance located on the ESXi/Hyper-V host then transferred to the recovery site to the paired VRA appliance in your recovery site where the write operation is placed into a journal. Checkpoints are recorded in the journal every few seconds, which allows you to failback to any point in time recorded in the journal's history with write order fidelity across all the virtual machines protected within that VPG. The journal length is configurable and directly relates to the amount of available checkpoints and storage consumption in the target environment.

RECOVERY DATA CENTERS

Workloads can be protected to the following US Signal data centers: Grand Rapids and Detroit, MI.

Workloads running in US Signal's enterprise cloud environment in one of these markets can either be protected to another US Signal data center or to your source data center.

REQUIRED COMPONENTS

+ Minimum dedicated bandwidth of 10 Mbps

+ Private MPLS or IPsec network connectivity between your source compute environment and recovery environment

VMWare

vCenter Server versions 4.1 or higher with at least one ESX/ESXi host.

Hyper-V

Microsoft System Center 2012 R2 with VMM and at least one Hyper-V host.

+ Only 2012 R2 Hyper-V hosts are supported

PLAYBOOKS

US Signal Professional Services Engineers will work with you to develop a customized DRaaS playbook, which includes all the necessary actions to failover the protected environment in the event of a disaster. Regular updates to the playbook are performed to ensure changes in your source environment are taken into account in your overall disaster recovery plan.

SERVICE LEVEL AGREEMENTS

For the Premium Tier of service, a SLA on the recovery time objective (RTO) will be established and documented in the customer's DRaaS playbook. RTOs range from minutes to hours. Actual achievable RTO will be derived through initial simulated failovers and are based on contingencies of the customer's environment size, bandwidth availablilty, or any other mitigating factors.

TESTING

Two free recovery tests per year are included to validate the viability of the recovery solution and ensure your DRaaS playbook is accurate. US Signal's Professional Services team will work with you to determine the testing scenario that meets your objectives.

DRaaS TIERS

US Signal's fully managed DRaaS solution is available in two service tiers — premium and standard — so customers can choose the level that's most appropriate for their specific applications, business requirements and budget.

Standard	Premium
Annual Testing **Included**	Annual Testing **Included**
Playbook Creation **Included**	Playbook Creation **Included**
Event Restoration Priority **Secondary**	Event Restoration Priority **Primary**
Storage Performance **Best Effort**	Storage Performance **Standard**
Resource Capacity Objective (RCapO) **Best Effort**	Resource Capacity Objective (RCapO) **100%**
RTO SLA **Best Effort**	RTO SLA **As Tested**