MANAGED CLOUD SERVICES - RECOVER FOR AWS - SERVICE GUIDE.

Last Modification Date: 08/06/2024
Exported and Shared on: 08/06/2024

For additional information, visit www.intervision.com

CONTENTS

1 MCS RECOVER OVERVIEW

1.1 SERVICE SUMMARY

InterVision MCS Recover proves your ability to recover mission-critical services at desired time intervals, from seconds to days, that maximizes efficiency and cost-effectiveness in a fully managed disaster recovery environment. InterVision's world-class support and implementation teams will work with the customer to determine the best recovery tier for each application/server. This managed service monitors and nurtures critical replication and recovery health components, providing insightful notifications to you and the InterVision service team to ensure recoverability is maintained. It also manages the testing and recovery process along with a team of disaster recovery experts to respond in a disaster.

Additional services may be added to support devices running in an MCS Recover environment, such as:

- Managed Firewall Services
- Managed Server
- Managed Endpoint Protection
- Backup as a Service

1.2 DRAAS SOLUTION SUITE FEATURES

The DRaaS solution suite offers the following features to optimize the replication environment:

- Cloud-native replication software, which includes:
- Application-aware processing: File, Systems, VMs, Database
- Data encryption for data in transit
- Data encryption for data at rest
- Reduction in stored data capacity and network traffic
- Unified billing for licensing, resources and support
- Configuration and management of the recovery storage and computing capacity required to run your protected workloads during the protection phase and additional resources to expand as needed within the specified RTO during the recovery state
- Network connectivity
- 24/7 Customer support
- Monitor and manage the replication and recovery infrastructure:
- Responding to alerts that are target infrastructure-related
- Performing software updates
- Configuration documentation and best practices to effectively manage your recovery needs
- Support for two annual, pre-scheduled test certifications initialized during standard support hours are included in the managed service as specified in the playbook testing section

- Professional services are available to help determine the workloads you need to have protected, assist with the creation of a playbook and test plans, and assist during tests and declarations as part of the implementation fee or through a paid consultation
- InterVision will initiate all actions defined in the Recovery Run Book. Services beyond the scope of the Run Book, including steady-state operations after the declaration, will require a separate statement of work and may incur additional professional service costs.

2 SERVICE DESCRIPTION

2.1 REPLICATION TARGETS

InterVision will create and manage the recovery environment that includes the resources (i.e. storage, network, and compute) to build the virtual targets as well as the necessary data mover technologies to successfully replicate to the recovery environment. The target should be somewhere in the same cloud ecosystem with a logical separation between the managed production environment and the DR environment.

The customer is responsible for all charges for the MCS Recover Environment. These charges are passed through to the customer on their InterVision invoice. Pricing indicated on the Service Order establishes a minimum monthly commitment. As changes occur and services are added, additional fees may be incurred.

Changes that incur extra charges may include but are not limited to:

- Adding VMs to replication
- Adding storage to replicated workloads
- Running workloads in the DRaaS Ready VDC
- Declaring a disaster
- Running a DR test
- Reverse Replication
- Support plans

Because clients are in control of their applications, virtual machines, and their replication, InterVision cannot guarantee an RPO for your specific workload.

2.2 REPLICATION CONNECTIVITY

InterVision will build the network connectivity during implementation between the MCS production environment and the MCS Recover environment.

2.3 RECOVERY PLAYBOOK AND TEST PLAN

A Disaster Recovery Playbook is a predefined staged task list to achieve recovery for disaster events. A Disaster Recovery Test Plan is similar to the Playbook but will include specific predefined staged task lists for isolation or specific testing scenarios that may differ somewhat from a real disaster declaration. These documents are developed during implementation and are maintained through subsequent testing events and customer notifications of necessary changes.

2.4 DISASTER RECOVERY TESTING AND DECLARATION

- Declarations will be treated as Priority 1 events
- Free test certifications must be scheduled at least 30 days in advance. Test initiation or support requested outside standard support hours will incur per-incident fees
- Additional services beyond initiating the test workflow will be billed on a time and material basis. Fees will be indicated in the playbook
- Upon test or declaration, existing and recovered VMs will be available for management and access through VPN or dedicated circuit
- All resources consumed during testing including compute, storage, IO, and data transfer are charged at current provider rates
- Additional services beyond initiating the test workflow will be billed on a time and material basis. Fees will be indicated in the playbook

2.5 CLIENT PORTAL

The following client portals are available to manage the client environment:

- AWS Management Console: Infrastructure management
- Microsoft Azure Portal: Infrastructure management

2.6 EXTENDED SERVICES

Optional Professional Services can provide the following support:

- Assessing workloads clients need to have protected
- Determining appropriate RPO targets
- Initial data seeding of recovery environments
- Assist with the creation of non-standard playbook and test plans

2.7 SERVICE DETAILS

The InterVision MCS Recover delivers the replication of production workloads to a DR environment in the same cloud ecosystem.

Monitoring and Support – InterVision will monitor the replication services to ensure that the service is running, remediate any issue related to InterVision-provided infrastructure, and provide reporting on any customer-impacting incidents. Monitoring information will be available to the customer via the client portal.

Service Playbook - InterVision will provide a DRaaS Service playbook template and assist with populating the playbook with information specific to the InterVision Recover Service.

Recovery Services - InterVision will assist with production site failover upon request by the customer. The InterVision service team will initiate the failover operations, monitor the failover activity, and validate that the virtual machines and workloads have been successfully failed over and are accessible. Tasks outside of the replication and failover are outside of the scope of this Service and can be provided under separate work orders. Application validation will be the customer's responsibility.

Service Portals – InterVision will provide access to the service portal for the following: service monitoring, administration, and for service requests.

Scheduled maintenance – Cloud architecture and software maintenance will be performed and communicated in standard maintenance windows.

2.8 ROLES & RESPONSIBILITY MATRIX

	Client	**InterVision**	**Extended Services***
General			
Server and Application information (account, password, location, etc.)	X		
Client escalation information	X		
Installation and Configuration			
Determine the data to be protected	X		X
Determine RPOs and RTOs for each application	X		X

Provide the restore information including System details, folder path and/or file, file overwrite, etc.	X		
Configuration of DR Side Software	X	X	
Install replication software	X		X
Create Replication Jobs	X	X	
Virtual target installation	X		
Physical IaaS target installation (excluding O/S)		X	
Physical non-standard target installation		X	X
Replication license		X	
Monitoring			
Monitoring of DRaaS Ready replication jobs		X	
Monitoring of DRaaS Restore replication jobs		X	X
Monitoring of non-standard targets			X
Incident and Problem Management			
Software and configuration support		X	
Event Notification		X	
Replication job issues	X	X	
Failover and recovery of protected systems**		X	
Failback planning and migration Post DR declaration			X

Malware and Ransomware removal	X		X
Maintenance and updates replication software		X	
Virtual target for agent-based replication	X		X
Physical IaaS target and infrastructure (firmware)		X	
Physical non-standard target and infrastructure (firmware, O/S, etc.)	X		X
Administer SW feature releases and non-critical updates		X	
Management			
Provide customer requirements (maintenance windows, reboot schedules, etc.)	X		
Administer user access to the portal	X	X	
Customer change management and notification	X		
InterVision notification of replication infrastructure maintenance events		X	
Reporting			
DR Playbook		X	
Custom Recovery Reports			X
Replication Policy Management – Post-Implementation			
Replication redesign			X
Disaster Recovery Playbook Updates		X	

- Extended Services are services that may be provided at a cost incremental to the monthly recurring fees.

2.9 SERVICE ACTIVATION

All implementations are treated as a project and owned by the InterVision Project Management Office. The Project Manager, Implementation Consultant, and Managed Cloud Services (MCS) member are the primary points of contact during the deployment of an MCS Recovery solution. Common step to service activation:

1. Project kickoff call with the client to introduce the project team, and understand requirements/key dates for the project.
2. Technical data gathering from the client.
3. Deployment of the client environment in the replication target
4. Review with the client how to connect to their environment.

2.10 COLLABORATIVE IMPLEMENTATION

1. Install appropriate replication technology in the client's production environment
2. Connecting client production environment to target repositories.
3. Initiate replication of client production workloads
4. Configuration of recovery firewall to match production configuration.
5. Upon completion of replication, a test plan is drafted for an initial DR test
6. The client performs a test of the DRaaS environment with our assistance.
7. Review findings with the client
8. Draft Playbook based on test plan and test findings
9. The playbook is revised until mutually agreeable.
10. Schedule Portfolio training with the client
11. Transition to steady-state operations with the Cloud Resiliency Team

InterVision recommends repeating steps 6-11 twice annually with the assistance of the InterVision Customer Support Team.

2.11 SERVICE ITEMS

SKU	Definitions
MCS Recover DR DevOps	DR Solution for DevOps Environment
MCS Recover DR Containers	DR Solution for Container based environment
MCS Recover DR Serverless	DR Solution for Serverless environment
MCS Recover DR Compute	DR Solution for Cloud based VMs

2.12 DEFINITIONS

Landing Zone: is a predefined operating environment designed and built for the purposes of supporting the InterVision service, providing the compute and network resources for recovery.

Client Content: Electronic data or information submitted by Client to the Disaster Recovery Service

Declaration: The announcement by preauthorized personnel that a disaster or severe outage has occurred (or is imminent) that triggers predefined response actions.

Declaration Event: The client has notified InterVision in writing (such as a support ticket) of intent to use the DRaaS VDC as the primary environment, i.e. to recover and resume production in the DRaaS VDC. Declaration Events are verified according to InterVision protocols.

DRaaS Runbook (Playbook): is a predefined staged task list to achieve recovery for disaster events. To be developed during disaster recovery testing.

DRaaS Virtual Data Center: and **DRaaS VDC:** shall mean an environment provided to Client by InterVision for purposes of replicating data and for recovering the virtual machines and data upon a Declaration Event. These are Run, Ready, and Restore VDC types.

Failback: the process of re-synchronizing that data back to the primary location, halting I/O and application activity once again, and cutting back over to the original location.

Failover: the process of shifting I/O and its processes from a primary location to a secondary disaster recovery (DR) location. This typically involves using a vendor's tool or a third-party tool of some type that can temporarily halt I/O, and restart it from a remote location.

Full Failover Test: An actual failover of the protected workload to the target site. Failback is needed to return the workload and any updates or transactions to its primary data center. A successful Sandbox Test is highly recommended before performing a Full Failover Test to reduce the risk of potential application disruption.

Journal: Contains the recovery checkpoints for the environment and stores continuous checkpoints for failover based on RPO and Retention settings.

Recovery Point Objective (RPO): point in time in which data must be recovered to avoid unacceptable data loss in a disaster situation.

Recovery Time Objective (RTO): is the target time for the recovery of your Virtual Machine after a disaster has struck. InterVision will validate that the virtual machine boots and operates. Client testing and validation that the application is operational is beyond the InterVision RTO.

Replication: is the Managed Service activity that manages and transfers the Client's data to the DRaaS VDC in a Replication State.

Replication Service: is the Managed Service about the replication activities and is a function of the number of Client Virtual Machines being replicated, or the amount of Storage consumed.

Recovery: The process of promoting a protected workload into full operation.

Recovery Test: is a test of the recovery processes and the DRaaS VDC environment in Recovery State that stops short of making it the primary production VDC for any period.

Recovery State: is the period between a Declaration Event and the time the Client has resumed production in the original primary environment or has converted the DRaaS VDC to a production VDC.

Sandbox Test: Allows for testing a copy of the protected workload in isolation at the target site with all updates or transactions being discarded upon completion.

Virtual Protection Group: A prioritized collection of Virtual Machines that must be recovered together

Zerto Cloud Appliance: Manages the three Zerto services within Amazon Web Services EC2 instance. The three services included in the Zerto Cloud Appliance:

- **Zerto Virtual Manager:** Manages disaster recovery, business continuity, and offsite backup functionality at the site level
- **Zerto Virtual Replication Appliance**: Replicates the VMs and virtual disks
- **Zerto Backup Appliance**: Manages offsite backup operations. Runs as a service at the target site, in this case, in Amazon Web Services, and enables the backup of replicated data. There is no host in ZCA.

2.13 DISASTER RECOVERY AS A SERVICE LEVEL OBJECTIVE

Recovery Service Level Objectives

Recovery Point Objective (RPO): The RPO will be determined by the Service Offering and the underlying technology architected to provide the solution. InterVision will perform the best effort to keep the RPO within the time specified in the customer's Playbook. The customer will be alerted should the solution fall out of the RPO set.

Recovery Time Objective (RTO): The RTO will be determined by the Service Offering and the underlying technology architected to provide the solution. The RTO SLO only applies to the Managed Service experiences. The RTO will be specified in the customer's Playbook, which will be developed during implementation.

The term **"Disaster Recovery Declaration"** is defined as follows:

A substantial outage of the Customer's IT infrastructure in which the Customer declares a disaster event. This Customer declaration activates the process of executing the Customer Disaster Recovery Plan documented in the InterVision DRaaS Runbook (Playbook). This DRaaS Runbook includes steps to transition primary Customer IT operations from the Primary location to the designated Disaster Recovery location.

InterVision will require a customer representative with a defined role of “Recovery” in the InterVision Portfolio Admin Tool to initiate the disaster declaration before creating a P1 ticket (emergency) for the event. Subsequent steps will be dictated by the Customer and following the Disaster Recovery Plan.