



DRAAS - SERVICE GUIDE V2

Last Modification Date: 06/07/2024
Exported and Shared on: 06/07/2024

For additional information, visit www.intervision.com

CONTENTS

| | | |
|----------|--|-----------|
| 1 | Service Summary | 1 |
| 1.1 | DRaaS Solution Suite Family | 1 |
| 1.2 | DRaaS Solution Suite Features..... | 1 |
| 2 | Service Description | 2 |
| 2.1 | Replication Targets | 2 |
| 2.2 | Replication Connectivity..... | 3 |
| 2.3 | Recovery Playbook and Test Plan | 3 |
| 2.4 | Disaster Recovery Testing and Declaration..... | 3 |
| 2.5 | Client Portal | 3 |
| 2.6 | Service Provider Portal..... | 3 |
| 2.7 | Extended Services..... | 4 |
| 3 | Service Details | 4 |
| 3.1 | Roles & Responsibility Matrix..... | 5 |
| 3.2 | Service Activation | 7 |
| 3.3 | Collaborative Implementation..... | 7 |
| 3.4 | Service Items..... | 8 |
| 3.5 | Definitions..... | 13 |
| 4 | DISASTER RECOVERY AS A SERVICE LEVEL OBJECTIVES AND COMMITMENTS | 15 |
| 4.1 | DRaaS Availability | 15 |
| 4.2 | Recovery Service Level Commitments..... | 15 |



4.3 DRaaS Service Credits for Declaration State 15

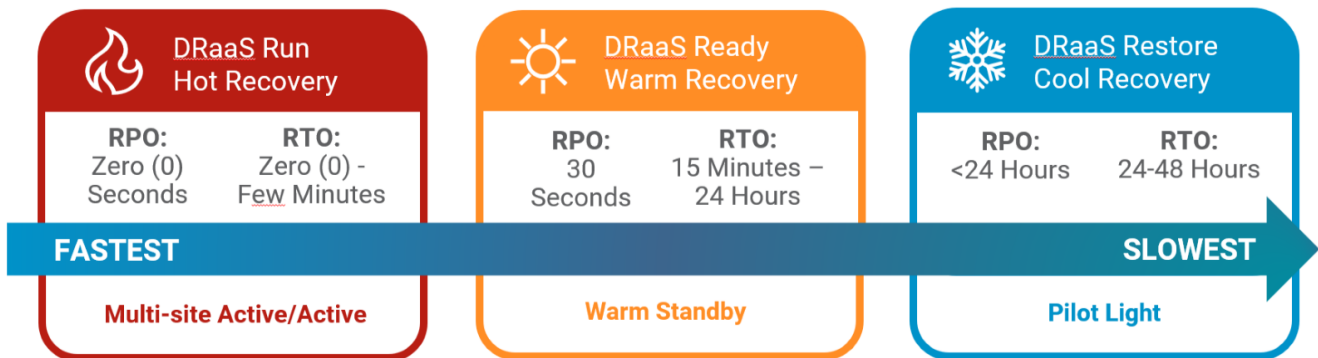
5 INFRASTRUCTURE AS A SERVICE AND DISASTER RECOVERY AS A SERVICE BILLING PROCEDURES..... 16

6 Change Log: Disaster Recovery as a Service (DRaaS) - Service Guide v2..... 17

1 SERVICE SUMMARY

InterVision DRaaS solution suite 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 what recovery tier works best for each specific 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.

1.1 DRAAS SOLUTION SUITE FAMILY



DRaaS Run™ proves your ability to recover your mission-critical services in near real-time. It combines the DRaaS managed recovery environment as an always-on virtual datacenter that runs a High Availability or passive replica of critical applications, servers, or services in a managed recovery environment.

Additional services may be added to support devices running in a DRaaS Run environment, such as:

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

DRaaS Ready™ proves your ability to recover your high-impact services within minutes to hours of a declaration. It protects the entire replicated application, both physical and virtual machines, in one recovery environment with fast RTOs and short RPOs.

DRaaS Restore™ proves your ability to recover your less critical services into the disaster recovery environment via offsite backups. This can also be a low-cost recovery alternative, perfect for important applications that lack the urgency of faster recovery time solutions.

Portfolio shows real-time and historic evidence of recoverability and certified test results to provide you with confidence and proof you can share with your stakeholders. You can also use Portfolio to review granular utilization and cost data, as well as configure alerts across the suite of DRaaS services in InterVision’s VMware powered cloud.

1.2 DRAAS SOLUTION SUITE FEATURES

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

- Enterprise-class replication software suite, 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 can work across Internet, VPN, and private circuits
- 24/7 Customer support
- Monitor and manage the replication and recovery infrastructure:
- Responding to alerts that are target infrastructure-related
- Performing software updates
- Client Portals to view replication jobs, policies, health information, and self-service capabilities
- 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 appliances to successfully replicate to the recovery environment. Multiple target environments are available for recovery such as hosted private cloud and public cloud.

RECOVERY SOLUTION TARGETS

On-Premises to Hosted
On-Premises to Public Cloud
Cloud Availability



The customer is responsible for all charges for the DRaaS Disaster Recovery 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 you are in control of your data center, 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 or will assist the customer in developing a connectivity plan per InterVision's recommendations.

Connectivity for DRaaS solutions includes one of the following as a standard offering:

- VPN
- Dedicated circuits
- End-to-end encryption powered by Veeam

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:

- Zerto Management Console: Replication management
- Veeam Backup & Replication Console: Replication and/or backup management
- Veeam Enterprise Manager: Reporting on replication and/or backups
- AWS Management Console: Infrastructure management
- Microsoft Azure Portal: Infrastructure management
- VMware vCloud Director: Infrastructure management
- Portfolio: ACF and playbook repository

2.6 SERVICE PROVIDER PORTAL

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



- Zerto Analytics: Reporting on replication
- Reports can be generated by the Service Provider and exported to Excel, CSV, or PDF
- Veeam Service Provider Portal: Management, reporting, and licensing

2.7 EXTENDED SERVICES

Optional Professional Services can provide the following support:

- Assessing workloads you 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
- Assist during non-standard tests and declarations as part of the implementation fee or through a paid consultation

3 SERVICE DETAILS

The InterVision Disaster Recovery as a Service (DRaaS) delivers the replication of virtual machines to an InterVision disaster recovery environment or to the public cloud.

Managed Virtual Machine Replication and Orchestration - InterVision utilizes 3rd party software to replicate, administer, and orchestrate the virtual machines and is available through the end-user web portal.

Monitoring and Support - InterVision will monitor the replication Service 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 Runbook - InterVision will provide a DRaaS Service runbook template and assist with populating the runbook with information specific to the InterVision DRaaS Service.

Disaster Recovery Service Validation - InterVision will provide a DRaaS Audit and Testing that provides the ability to validate replication and failover services. The validation Service includes reviews of customer-specific documentation and runbook and target recovery resource pool and site-to-site connectivity. VM failover services will be tested. InterVision will provide a report of the failover readiness and consult of potential issues and recommendations. This Service is an additional fee and is required to maintain the service SLO and SLA promises to ensure the SLO and SLA can be met.

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

Service Portals - InterVision will provide access to service portal for the following: service monitoring, VM administration, and for service request.

Scheduled Maintenance - Infrastructure and Software maintenance will be performed and communicated in standard maintenance windows.

Initial data seeding services - are available for an additional fee. Contact InterVision's Professional Services for details and pricing information.



3.1 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 | |



DRAAS - SERVICE GUIDE V2

| | | | |
|---|---|---|---|
| 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 | | | |



DRAAS - SERVICE GUIDE V2

| | | | |
|---|---|---|---|
| Provide customer requirements (maintenance windows, reboot schedules, etc.) | X | | |
| Administer user access to 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.

**May require additional professional services fees for a disaster declaration. or testing outside of standard support hours.

3.2 SERVICE ACTIVATION

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

1. Project kickoff call with the client to introduce the project team, 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.

3.3 COLLABORATIVE IMPLEMENTATION

1. Install appropriate replication technology in the client's production environment
2. Connecting client production environment to target (typically a VPN or dedicated PtoP)
3. Initiate replication of client Virtual Machines



DRAAS - SERVICE GUIDE V2

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 test of 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 Cloud Resiliency Team

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

3.4 SERVICE ITEMS

The following service items may be included when purchasing the DRaaS Solution suite.

| DRaaS RUN VDC SKUs | Definitions |
|---|--|
| RUN CPU - vCPU - Zone 2 | Powered on vCPU. For example, an actively powered on VM such as a firewall or load balancer, or an active-active VM using native replication |
| RUN CPU - vCPU - Zone 1 | |
| RUN Memory - GB - Zone 2 | Powered on Memory. For example, an actively powered on VM such as a firewall or load balancer, or an active-active VM using native replication |
| RUN Memory - GB - Zone 1 | |
| RUN Storage - Standard Encrypted - GB- Zone 2 | Total storage provisioned for powered on or powered off workloads. This is NOT storage reserved for time of recovery. |
| RUN Storage - Standard Encrypted - GB- Zone 1 | |
| RUN Internet - GB- Minimum -Zone 2 | Minimum Internet Charge |
| RUN Internet - GB- Minimum -Zone 1 | |
| RUN Internet - GB- Zone 2 | Total transferred data for ingress and egress |
| RUN Internet - GB- Zone 1 | |
| RUN IP Address - Each- Zone 2 | IP addresses |
| RUN IP Address - Each- Zone 1 | |
| RUN Contracted VDC Support | Support for Disaster Recovery Virtual Datacenter |



DRAAS - SERVICE GUIDE V2

| | |
|---|---|
| RUN CPU at Recovery- Each- Zone 2 | Reserved CPU availability for non powered on workloads at recovery. For example, a VM that gets cloned at the time of recovery, such as multiple RDS server. |
| RUN CPU at Recovery- Each- Zone 1 | |
| RUN Memory at Recovery- GB- Zone 2 | Reserved Memory availability for non powered on workloads at recovery. For example, a preconfigured firewall or load balancer that remains powered off until the time of recovery. |
| RUN Memory at Recovery- GB- Zone 1 | |
| RUN Storage - Standard at Recovery - GB- Zone 2 | Reserved Storage availability for non powered on workloads at recovery. For example, a preconfigured firewall or load balancer that remains powered off until the time of recovery. |
| RUN Storage - Standard at Recovery - GB- Zone 1 | |
| | |
| DRaaS Ready VDC SKUs | Definitions |
| READY Storage DRaaS Ready - GB - Zone 2 | Replicated Provisioned Storage. This is storage utilized by replication (Journal and volumes), NOT recovered workloads. |
| READY Storage DRaaS Ready - GB - Zone 1 | |
| READY Internet - GB - Minimum - Zone 2 | Minimum Internet Charge |
| READY Internet - GB - Minimum - Zone 1 | |
| READY Internet - GB - Zone 2 | Internet Bandwidth Consumption |
| READY Internet - GB - Zone 1 | |
| READY IP Address - Each- Zone 2 | IP addresses |
| READY IP Address - Each- Zone 1 | |
| READY Contracted VDC Support | Support for Disaster Recovery Virtual Datacenter |
| AWS Contracted VDC Support | |
| Azure Contracted VDC Support | |



DRAAS - SERVICE GUIDE V2

| | |
|---|--|
| READY DRaaS Managed Services - Replication Service - Ready Virtual - Zone 2 | Managed Service for the replication technology |
| READY DRaaS Managed Services - Replication Service - Ready Virtual - Zone 1 | |
| READY DRaaS Managed Services - Replication Service - Ready Virtual - AWS | |
| READY DRaaS Managed Services - Replication Service - Ready Virtual - Azure | |
| AWS eDRS Replication Service Ready Virtual | |
| Azure ASR Replication Service - Ready Virtual | |
| AWS Storage Replication Service | Managed Service for the replication of cloud storage |
| Azure Storage Replication Service | |
| AWS DB Replication Service | Managed Service for the replication of cloud database services |
| Azure DB Replication Service | |
| READY TO CPU at Recovery- Each - Zone 2 | Reserved vCPU availability for replicated workloads. This is vCPU utilized by workloads upon recovery. |
| READY TO CPU at Recovery- Each - Zone 1 | |
| READY TO Memory at Recovery- GB- Ready-To - Zone 2 | Reserved Memory availability for replicated workloads. This is memory utilized by workloads upon recovery. |
| READY TO Memory at Recovery- GB- Ready-To - Zone 1 | |
| READY TO Storage Standard at Recovery- GB - Zone 2 | Reserved Storage availability for replicated workloads. This is storage utilized by workloads upon recovery. |
| READY TO Storage Standard at Recovery- GB - Zone 1 | |
| READY DRaaS Managed Services - Max Bandwidth at Rec | This is an Internet bandwidth increase upon failover |



DRAAS - SERVICE GUIDE V2

| | |
|---|---|
| READY License - DRaaS Replication - Zone 2 | Software License for DRaaS Ready Replication using Zerto, billed per VM. |
| READY License - DRaaS Replication - Zone 1 | |
| | |
| DRaaS Restore VDC SKUs | Definitions |
| RESTORE Storage GB - Zone 2 | Backup Repo Consumed Storage. This is storage utilized by full and incremental backups, NOT recovered workloads. |
| RESTORE Storage GB - Zone 1 | |
| RESTORE Internet - GB- Minimum -Zone 2 | Minimum Internet Charge |
| RESTORE Internet - GB- Minimum -Zone 1 | |
| RESTORE Internet - GB- Zone 2 | Internet Bandwidth Consumption |
| RESTORE Internet - GB- Zone 1 | |
| RESTORE IP Address - Each- Zone 2 | IP addresses |
| RESTORE IP Address - Each- Zone 1 | |
| RESTORE Contracted VDC Support | Support for Disaster Recovery Virtual Datacenter |
| RESTORE DRaaS Managed Services - Replication Service - Zone 2 | Storage based managed service fee, billed per GB. This is the amount of storage we are protecting. |
| RESTORE DRaaS Managed Services - Replication Service - Zone 1 | |
| RESTORE DRaaS Managed Services - Replication Service - AWS | |
| RESTORE DRaaS Managed Services - Replication Service - Azure | |
| Replication Service - Restore Mgd Service per VM - Zone 2 | Device based managed service fee, billed per device (VM or agent). This is the number of devices we are protecting. |



DRAAS - SERVICE GUIDE V2

| | |
|---|---|
| Replication Service - Restore Mgd Service per VM - Zone 1 | |
| Replication Service - Restore Mgd Service per VM - AWS | |
| Replication Service - Restore Mgd Service per VM - Azure | |
| RESTORE CPU at Recovery- Each- Zone 2 | Reserved vCPU availability for replicated workloads. This is vCPU utilized by workloads upon recovery. |
| RESTORE CPU at Recovery- Each- Zone 1 | |
| RESTORE Memory at Recovery- GB- Zone 2 | Reserved Memory availability for replicated workloads. This is memory utilized by workloads upon recovery. |
| RESTORE Memory at Recovery- GB- Zone 1 | |
| RESTORE Storage - Standard at Recovery - GB- Zone 2 | Reserved Storage availability for replicated workloads. This is storage utilized by workloads upon recovery. |
| RESTORE Storage - Standard at Recovery - GB- Zone 1 | |
| RESTORE DRaaS Managed Services - Max Bandwidth at Rec - 10 Mb | This is an Internet bandwidth increase upon failover |
| | |
| Cloud Consumption Spend | Definitions |
| AWS Managed Resiliency VPC Landing Zone | Captures total cloud consumption spend of your DRaaS Disaster Recovery Environment. This is the charge received on the AWS/Azure bill and passed through to the customer. |
| Azure Managed Resiliency Landing Zone | |
| | |
| RPaaS Ransomware Recovery | Definitions |
| Resiliency Server Protection (License + Managed Service) | Stand alone Veeam license and Managed Service fee, NOT part of RPaaS bundle |



DRAAS - SERVICE GUIDE V2

| | |
|---|---|
| Resiliency Server Protection (BYOL + Managed Service) | Stand alone BYOL Veeam license and Managed Service fee, NOT part of RPaaS bundle |
| RPaaS Resiliency Server Protection (License + Managed Service) | RPaaS bundled Veeam license and Managed Service fee based on per device |
| RPaaS Resiliency Server Protection (BYOL + Managed Service) | RPaaS bundled BYOL Veeam license and Managed Service fee based on per device |
| RPaaS Resiliency Storage Protection (License + Managed Service) | RPaaS bundled Veeam license and Managed Service fee based on per GB of storage |
| RPaaS Resiliency Storage Protection (BYOL + Managed Service) | RPaaS bundled BYOL Veeam license and Managed Service fee based on per GB of storage |
| RPaaS O365 Resiliency | RPaaS bundled Veeam license and Managed Service fee for O365 based on per user |
| | |
| Business Continuity and VDC Support | Definitions |
| AWS VPC Landing Zone (variable cost) | AWS environment where backups are stored and/or where cloud recovery occurs. Cost is determined by monthly resources utilized and passed directly through to the customer |
| Azure Landing Zone (variable cost) | Azure environment where backups are stored and/or where cloud recovery occurs. Cost is determined by monthly resources utilized and passed directly through to the customer |
| Contracted VDC Support (variable cost) | Support costs are based on a percentage of monthly utilization (see landing zones above) |

3.5 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.



DRAAS - SERVICE GUIDE V2

Declaration Event: is 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 datacenter. 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, 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 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 pertaining to 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.



4 DISASTER RECOVERY AS A SERVICE LEVEL OBJECTIVES AND COMMITMENTS

4.1 DRAAS AVAILABILITY

InterVision commits that the DRaaS Infrastructure will be available 99.99% in a given calendar month. Should the DRaaS Service Monthly Availability fall below 99.99%, Service Credits are defined in the Work Order

InterVision commits that the DRaaS Services will be available 99.9% in a given calendar month. Should the DRaaS Service Monthly Availability fall below 99.99%, Service Credits are defined in the Work Order

DRaaS Monthly Availability % is calculated per Data Center on a monthly basis, as: $100\% - (\text{Total DRaaS downtime minutes, divided by total minutes in a given month.})$ Downtime minutes are accrued starting after the first 20 minutes during which the DRaaS was reported as inaccessible. Service Credits will be applied only for the portion of the BaaS that was affected and unavailable.

4.2 RECOVERY SERVICE LEVEL COMMITMENTS

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 developed during implementation.

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

A substantial outage of the Customer IT infrastructure in which the Customer declares a disaster event. This Customer declaration activates the process to execute 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 prior to creating a P1 ticket (emergency) for the event. Subsequent steps will be dictated by the Customer and in accordance with the Disaster Recovery Plan.

4.3 DRAAS SERVICE CREDITS FOR DECLARATION STATE

When a client invokes a Disaster Recovery Declaration Event for a DRaaS VDC into a vCloud environment, (i.e. Run, Ready, and Restore); the IaaS Premium Service Level Objectives and Service Level Commitments apply and all resources within the contracted capacity specified in the Sales Order will be available and all Virtual Machines that can recover within the contracted capacity will be powered on unless otherwise specified.

Exclusions

The following are not covered by this SLO:

- The customer is solely responsible for generating and formatting all data.
- The customer is solely responsible for the integrity of all data targeted for DRaaS.
- Failure of the customer's Internet or other network connection to the DRaaS servers (e.g. via the public Internet or the customer's network).
- Malfunction of customer's computing systems upon which the DRaaS components are installed (including hardware, operating system(s), or local software) – including lack of availability due to configuration issues.



- Inability to access DRaaS due to customer security or software provided by customer or 3rd
- For DRaaS products that target AWS for their recovery: 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.

5 INFRASTRUCTURE AS A SERVICE AND DISASTER RECOVERY AS A SERVICE BILLING PROCEDURES

InterVision shall invoice the Client monthly in advance for the Monthly Minimum Fee for each VDC in the Client Environment.

Following each billing period, InterVision shall compute the Actual Usage for each VDC in the Client Environment as described for each component type below. InterVision shall compute any Additional Use and the Additional Use Spend. InterVision shall invoice Client monthly in arrears for any Additional Use Spend. If Actual Usage is lower than the Monthly Minimum Fee, there is no refund of or credit for the Monthly Minimum Fee billed in advance.

Actual Usage for infrastructure components is calculated as follows.

CPU usage is calculated as the sum of the daily CPU usage for each Day in the Billing Period where the daily CPU usage is the maximum Sampled CPU value for that Day multiplied by the daily rate for CPU shown in the Rate Schedule.

- Memory usage is calculated as the sum of the Memory daily usage for each Day in the Billing Period where the daily Memory usage is the maximum Sampled Memory value for that Day multiplied by the daily rate for Memory shown in the Rate Schedule.
- Storage usage is calculated as the sum of the Storage daily usage for each Day in the Billing Period where the daily Storage usage is the maximum Sampled Storage value for each type of Storage for that Day multiplied by the daily rate for that specific type of Storage shown in the Rate Schedule.
- Internet usage is calculated as the sum of the number of Gigabytes sent and received via InterVision's internet service for that Day multiplied by the daily rate for the Internet shown in the Rate Schedule.
- Port Data Flow usage is calculated as the sum of the number of Gigabytes sent and received through a Port dedicated to the Client for that Day multiplied by the daily rate for Port Data Flow shown in the Rate Schedule.
- IP Address usage is calculated as the sum of the IP Address daily usage for each Day in the Billing Period where the daily IP Address usage is the number of IP Addresses assigned for that Day multiplied by the daily rate for IP Address shown in the Rate Schedule.

Support usage is calculated as the applicable percentage of total Infrastructure Component Actual Usage Fees incurred in the Billing Period. The applicable percentage is shown on the Sales Order for each VDC.

Actual Usage for Managed Service components is calculated as follows.

The Replication Service associated with DRaaS Ready VDCs is calculated as the sum of the daily VM replication usage for each Day in the Billing Period where the daily VM replication usage is the maximum value of Sampled VMs being replicated for that Day multiplied by the daily rate for Replication Service shown in the Rate Schedule. For clarity, the daily rate does not change based on the number of VMs being replicated; it is established based on the number of VMs on the Service order and used to calculate the Monthly Minimum Fee.

The Replication Service associated with DRaaS Restore VDCs is calculated as the sum of the daily Storage usage for each Day in the Billing Period where the daily Storage usage is the maximum value of Sampled Storage being consumed for that Day multiplied by the daily rate for Replication Service shown in the Rate Schedule. For clarity, the daily rate does not change based on Storage consumption; it is established based on the Storage value on the Service order and used to calculate the Monthly Minimum Fee.

Managed Services associated with DRaaS VDC at-recovery items (e.g. CPU at Recovery, Memory at Recovery, Max Bandwidth at Recovery and Storage at Recovery) are calculated for each service ordered as the sum of the at-



DRAAS - SERVICE GUIDE V2

recovery Managed Service amount shown on the Service order multiplied by the daily rate for the specific Managed Service shown in the Rate Schedule.

License usage is calculated for each type of License as the maximum, concurrent number of license units, typically a one per virtual machines (VM) or one per CPU in the VM, with the License provisioned, whether the associated VM is powered- on or powered-off, at each point in the Billing Period (also described as the “High Water Mark”) multiplied by the monthly rate for the License shown in the Rate Schedule. Each “Copy” action counts as an instance. A “Move”, which is technically a copy and delete, is counted only as a single instance.

Eligible Microsoft Windows Server Applications (e.g. Microsoft SQL Server Standard Edition) deployed in the InterVision VDC that are covered by an existing application license will not be included in the calculation. This option is available to Microsoft Volume Licensing (VL) customers with eligible server applications covered by active Microsoft Software Assurance (SA) contracts. Information on the required verification is available from Microsoft. InterVision must have documentation showing the Client’s eligibility under Microsoft Software Assurance or Client is responsible for license fees.

Professional Services are measured monthly during the billing period as described in the corresponding Work Order.

Recovery State billing

1. If Client has authorized Professional Services for PlayBook execution or other Professional Services specified in a separate statement of work, InterVision will perform the services and invoice for those services upon Declaration Event.
2. Usage for Bandwidth, CPU, and Memory and other Resource during the Recovery State will be invoiced as described above for Premium VDCs. Other usage fees may include Managed Services, Support, and License fees if those resources apply in the primary VDC. These other usage fees are charged at the primary VDC rate or, if they are needed and not in the primary VDC, they will be charged at the then-current Premium VDC rates. Usage fees will continue until the authorized decommissioning or return to Replication State.

Declaration Test billing

1. For Declaration Tests scheduled by Client and confirmed by InterVision, Declaration Test Infrastructure Resources will be credited for up to three Days each two times annually. Annual periods commence on the Initial Start Term.
2. Professional Services authorized by Client, if any, will apply.

Per Incident support fees are in addition to the standard Support Fee and are invoiced only when authorized by Client for specific, out-of-scope support activities.

6 CHANGE LOG: DISASTER RECOVERY AS A SERVICE (DRAAS) - SERVICE GUIDE V2

Below are the changes to this service guide.

| Change date | Change Type | Change Details |
|--------------|--------------|--|
| May 1, 2024 | New Document | Initial release |
| June 7, 2024 | SKU Updates | Updated SKUs for Landing Zones and VDC Support |

