Disaster Recovery-as-a-Service

Product E-Book

CBTS

TECHNOLOGY SOLUTIONS FOR BUSINESS

Table of Contents

Product Overview

IT departments invest in various ways to recover from a disaster. Disasters can be small-scale, like equipment or network failure; medium-scale, like a complete data center outage; or large-scale, like a natural event.

Historically IT organizations have had two options:

1. **Stand-up a Disaster Recovery (DR) data center, replicate data to it and failover when needed**. This is an expensive proposition as the DR equipment must match to the production workloads and the equipment sits mostly idle. Some organizations justify the cost of this equipment by running test and dev workloads, but there is no return or very little return on investment until an actual disaster occurs.
2. **Replicate your production workloads to a cloud provider**. Large cloud providers do not provide any services, so you are left on your own to perform all disaster recovery tests, failover the production environment to the cloud provider, and then figure out how to failback once the outage has been repaired.

The CBTS Disaster Recovery-as-a-Service (DRaaS) solution gives you the benefits of utilizing the cloud, and includes management and support from CBTS. It is a multi-tenant disaster recovery solution that enables you to replicate virtual machines (VMs) from your source environment to a geographically-separate DR target environment hosted by CBTS.

This solution consists of the following components:

- Network
- Storage resources
- Compute resources
- Disaster recovery orchestration
- Monitored DR target environment infrastructure
- People (system admin) & Process

Our DRaaS solution is engineered to be a critical component of your overall business continuity planning (BCP) process.

Benefits

There are a number of benefits to using our DRaaS solution:

- **Better Utilize Your Own Resources**
  You no longer need a separate DR data center. Allocate all of your computing resources towards running your business instead of having them sit idle.

- **Simple Monthly Pricing**
  Easy-to-understand pricing lets you know your charges up front and turns capital expense (CapEx) to operational expense (OpEx). The utility service model eliminates capital outlay and allows customers to pay a monthly fee. Plus, you can grow as needed without purchasing multi-year capacity up front.

- **Full Flexibility**
  This solution allows you to utilize resources as you need them and only purchase those you need without spending more. Our "as-a-Service" model allows for predictable spending based on your overall DR requirements.

- **Excellent Reliability**
  CBTS is known for reliability. Our highly-trained data protection engineers monitor and manage the environment from our Enterprise Network Operations Center (ENOC) 24 hours a day, 7 days a week, 365 days a year.

Additional Benefits

Our solution makes it easier to meet compliance requirements, such as those to which financial institutions must adhere, and is supported by a strong technology foundation from industry-leading companies. It is well tested and proven to work in almost any environment, with all data encrypted in-flight and at-rest. This is in contrast to solutions from some other providers that are developed in house. We can provide orchestration for DR testing and failovers, including power on orders, failover groups, pre & post scripts, etc. It offers multiple restore points to allow the flexibility to have multiple Recovery Point Objectives (RPOs*). Engineering assistance is available for scheduled DR tests as well as in case of an actual disaster and includes firewall services and public IP address assignments. Multiple connectivity options to connect to the CBTS data center are offered, including over the Internet, IP VPN, etc.

Pricing Overview

This service is priced as follows:

- Monthly billing is based on the number of VMs plus consumed storage.
- If powered on, billing is based on CPU, memory and storage assigned to VM.
- Installation fee is charged per server.
- Optional engineering resources are charged on a time and materials basis.

Product Details

DRaaS utilizes software-based replication to protect the customer's source environment. In a DR event or test, the protected source machines are recovered in a target environment managed by CBTS. Recovery consists of powering on replicated machines, and access (or remote access) to the replicated machines.

CBTS' DRaaS integrates computing resources and VM replication software, as well as strict IT processes and governance based on the Information Technology Infrastructure Library (ITIL) model. CBTS' engineers ensure that the target environment network, remote access drives and related DRaaS infrastructure are available according to the Availability Service Level Agreement (SLA).

CBTS will provide and maintain each of the following for the DRaaS target environment:

- Virtual CPU and RAM for replicated VMs
- Storage components for replicated VMs
- SSL VPN client connectivity for remote access of recovered VMs in a DR test or DR event
- All data center power, cooling, and operations to support DRaaS target infrastructure
- DR software licensing and infrastructure for replication
- DR orchestration, which automates VM recovery order based on customer-determined business criticality and dependencies

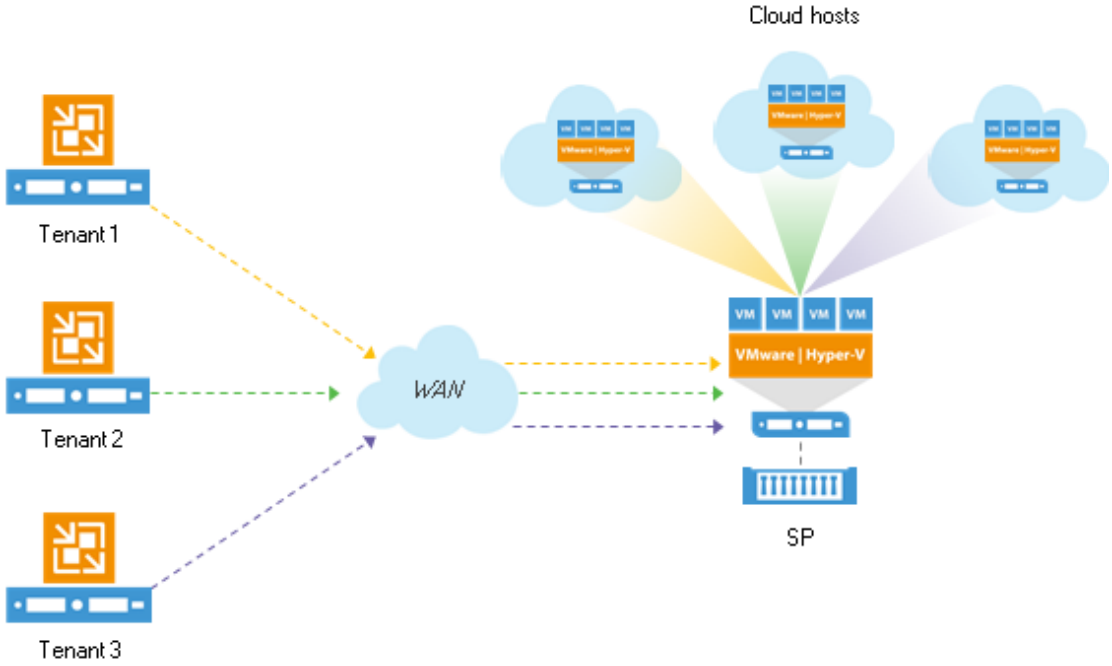
Customers will be responsible for ensuring that the source environment meets certain requirements to enable DRaaS including, but not limited to:

- Network connectivity
- VMware virtual infrastructure
- Monitoring and troubleshooting of DR replication

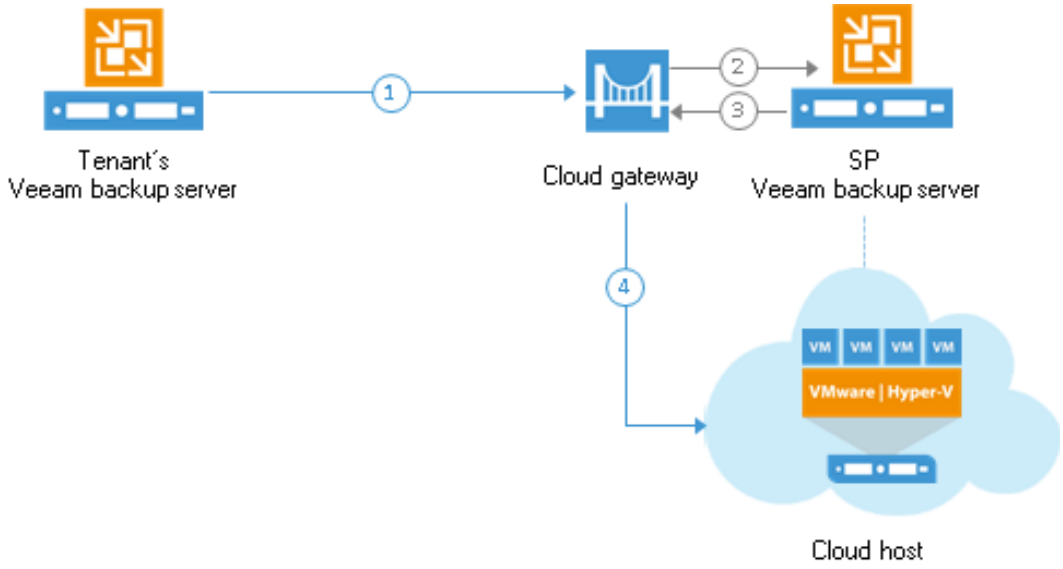
CBTS has data centers in Cincinnati (Ohio), Hamilton (Ohio) and Carrollton (Texas). The DRaaS target environment will be placed in a geographically diverse location.

Architecture

DRaaS connection over WAN



DRaaS connection over the Internet using Cloud Gateway



Security

Our DRaaS cloud is hosted in a secure datacenter with SSAE16 certification. Security features include:

- Data at rest encryption for DRaaS storage
- Replication traffic encrypted using AES 256-bit encryption
- Secure connectivity to CBTS DRaaS Cloud
- Firewall between networks in DRaaS target environment
- DRaaS infrastructure securely maintained and monitored, including patching, anti-malware, monitoring, log collection, and vulnerability scanning

SKU Detail

Product/Service	Description	Charge Frequency
Install/Setup	Setup of DRaaS in the customer's environment, which includes installation of replication software on customer site and assistance with configuring replication software.	Per Server
Standby Replica VM	VM that is not consuming CPU/memory resources and is protected. Source and target licensing is included (replication licenses only).	Per VM/month
Replicated Storage	Storage associated to the cold standby replica VM, including VM disks and restore points.	Per GB/month
Recovered DR VM	A running, recovered VM during a test or failover. VMW are licenses included.	Per day
Engineering Services	Time and material for DRaaS-related support and services, including assistance with DR testing/failover plan, addition of new network/machines/resources, and changes to advisory board participation.	Per 15 minutes

The following services are included:

Monitoring

- Continual system availability monitoring using standard platform management tools

DRaaS Administration

- Administration of underlying infrastructure
- Skilled engineers capable of diagnosing and resolving most service disruptions

Network Switching and Firewall Infrastructure

- Enterprise firewall and switching infrastructure, maintenance, monitoring, and hardware for all CBTS-hosted DR infrastructure

Advanced Enterprise Reporting

- Advanced reporting that allows verification of service levels and recoverability

Service Level Agreements (SLAs)

CBTS' DRaaS target environment is designed to meet **the Recovery Point Objective (RPO)** and the **Recovery Time Objective (RTO)**.

RPO is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure.

RPO is greatly affected by the source environment and the rate of data change. CBTS has designed the service to meet the RPO of **fifteen (15) minutes**. At that same time, the customer must ensure that the daily data change rate is consistent after the initial seed, and that the customer has sufficient bandwidth to replicate the daily data change rate.

The **RTO** is the targeted duration of time and a service level within which a business process must be restored in order to avoid unacceptable consequences associated with a break in business continuity.

CBTS will use reasonable efforts to ensure that the DRaaS environment can support an average startup rate of **approximately one and a quarter (1.25) virtual guest Operating Systems per minute, or seventy-five (75) virtual guests per hour**.

Service is provided to the DRaaS environment with a **99.9% availability guarantee** in a monthly measure. Availability is measured as the percentage of time the underlying DR target environment is accessible during a given month. An "outage" occurs when the underlying DR target infrastructure is unavailable to replicate the source environment.

For these SLAs to remain in effect, CBTS requires that the customer conduct, at minimum, two (2) DR tests per year in order to assess the DRaaS RPO and RTO, and to remediate accordingly. CBTS and the customer will jointly review DR test results and CBTS will make all reasonable changes requested by the customer to maintain RTO and RPO.

Reporting

The following reports are provided with the DRaaS solution:

Report Name	*Description*	*Standard Publication Schedule*
DR Execution Evidence	Provide evidence to customer of the execution steps performed by the DR software during Failover Execution to meet Customer Compliance Requirements	Per customer request
Incident Management Responsiveness	This is the time between alarm and ticket creation.	Monthly
Service Request Timeliness	This is the time between service request opened and service request closed (less pause time if applicable).	Monthly
MTTR (Mean-Time to Repair)	This is the time between alarm and incident closed (less pause time if applicable).	Monthly

Roles and Responsibilities Matrix

Responsibilities	*CBTS*	*Customer*
DRaaS infrastructure preventative maintenance – firmware updates; compute network and storage (not Guest systems)	X	
DRaaS infrastructure capacity management	X	
DRaaS environment hypervisor license management	X	
Hardware licensing related to delivering VMs (multi-pathing for storage networking, networking hardware, compute hardware, storage hardware)	X	
Source-side DR software maintenance and licensing when procured through CBTS in the Agreement or a Related Agreement	X	
Target-side DR software maintenance and licensing	X	
Operating System Client access licenses or remote desktop licenses where source environment is CBTS Infrastructure-as-a-Service	X	
Replicated VM OS licenses – Windows and Red Hat Enterprise Linux		X
Operating System Client access licenses or remote desktop licenses where the customer owns the source environment		X

Networking between the customer's network(s) and the VDC firewalls		X
Customer-procured source-side DR software maintenance and licensing		X
Guest (VM) IP management		X
Application software licenses		X
Security/security audits and compliance		X
Infrastructure applications (Active Directory domains, DNS, DHCP management, WINS, etc.)		X
Determine and inform CBTS of virtual server criticality for DR Orchestration (power on order, RPO/RTO, etc.)		X
Comprehensive business continuity planning		X
DR planning and preparation		X
DR test request and scheduling (to be mutually agreed upon)		X
Validate DR testing: evaluate and act upon results and remediation		X
DNS updates		X
DR declaration for both DR tests and DR events		X

Management Responsibility Definitions

Capacity Reporting and Management ensures that the capacity of IT services and the IT infrastructure is able to deliver agreed Service Level Targets in a cost-effective and timely manner. This process considers all resources required to deliver the IT services, and plans for short-, medium- and long-term business requirements.

Incident Management deals with all incidents, including failures, questions or queries reported by the users (usually via a telephone call to the Service Desk), technical staff, or automatically detected and reported by event monitoring tools.

Change Management controls the lifecycle of all changes with the primary objective to enable beneficial changes to be made, with minimum disruption to IT services.

Routine Configuration Management is a part of an overall Service Asset and Configuration Management Process and responsible for maintaining information about Configuration Items (CI) required to deliver an IT service, including their relationships. The information is managed throughout the lifecycle of the CI.

Problem Management administers the lifecycle of all problems and is provided to prevent incidents and minimize the impact of incidents that cannot be prevented.

Proactive Problem Management analyzes Incident Records, and uses data collected by other IT Service Management processes to identify trends or significant problems.

Continuous Improvements are identified to ensure that services are aligned with the customer's changing business needs. The process includes operational reviews, root cause analysis, documentation updates and best practices to measure performance.