Contents

Introduction .................................................................................................................. 6
  1.1 Overview .............................................................................................................. 6
  1.2 vCloud Availability Cloud-to-Cloud DR Workflow ........................................... 6
  1.3 VMware vCloud Availability for Cloud-to-Cloud DR Features ......................... 7

Use Cases .................................................................................................................... 8
  2.1 Migration ............................................................................................................ 8
  2.2 Disaster Recovery ............................................................................................. 8
  2.3 Disaster Avoidance ........................................................................................... 8
  2.4 Upgrade and Patch Testing .............................................................................. 8

vCloud Availability Cloud-to-Cloud DR Components ................................................. 9
  3.1 vSphere Replication Server and vSphere Replication Filter ............................... 9
  3.2 vCloud Availability Replicator .......................................................................... 9
  3.3 vCloud Availability Replication Manager ......................................................... 9
  3.4 vCloud Availability vApp Replication Service/Manager ...................................... 9
  3.5 Light Weight Delta Protocol (LWD Proxy) ......................................................... 9
  3.6 vCloud Availability Tunnel ............................................................................... 10
  3.7 vCloud Availability for Cloud-to-Cloud DR portal ........................................... 10

vCloud Availability Cloud-to-Cloud DR Node Types and Sizing .............................. 11
  4.1 Node Deployment Types (Service Provider Components): ............................... 11
  4.2 Node Sizing: ...................................................................................................... 11
  4.3 vCloud Availability Cloud-to-Cloud DR Operational Limits: ............................ 12

vCloud Availability Cloud-to-Cloud DR Deployment Requirements .................... 12
  5.1 VMware vCloud Director and SSO ................................................................. 12
  5.2 Network Requirements .................................................................................... 12
  5.3 Replication and Network Bandwidth Requirements ......................................... 13

vCloud Availability Cloud-to-Cloud DR Architecture Design ............................... 15
  6.1 vCloud Availability Cloud-to-Cloud DR Conceptual Design ............................ 15
  6.2 vCloud Availability Cloud-to-Cloud DR Logical Design .................................. 16
  6.3 Servers for vCloud Availability Cloud-to-Cloud DR without Tunnel Appliance ........................................................................................................ 16
  6.4 Servers for vCloud Availability Cloud-to-Cloud DR with Tunnel Appliance .... 16
  6.5 High Availability for vCloud Availability Cloud-to-Cloud DR ......................... 17
  6.6 Minimum High Availability Component for vCloud Availability Cloud-to-Cloud DR........ 17

Physical Design .......................................................................................................... 20
7.1 vCloud Availability Cloud-to-Cloud DR Sites and Locations ........................................... 20
7.2 vCloud Availability Cloud-to-Cloud DR deployment without tunnel appliance .......... 20
7.3 vCloud Availability Cloud-to-Cloud DR deployment with tunnel appliance ............... 21
7.4 Replace vCloud Availability vApp Replication Manager Certificate with a CA Signed Certificate .......................................................... 21

Network Communication and Firewalls ................................................................. 22
8.1 Network Ports for Local Site Connection Without Cloud-to-Cloud Tunneling .......... 22
8.2 Network Ports for External Communication Without Cloud-to-Cloud Tunneling .... 24
8.3 Network Ports for Internal Communication with Cloud-to-Cloud Tunneling .......... 25
8.4 Network Ports for External Communication with Cloud-to-Cloud Tunneling .......... 27

Deployment ........................................................................................................... 28
9.1 Deploy vCloud Availability Cloud-to-Cloud DR OVA ................................................. 28
Follow these Steps for each Sites ................................................................. 28
9.2 Configure vCloud Availability Cloud-to-Cloud DR Replicator ................................. 29
9.3 Configure a vCloud Availability Replication Manager ............................................. 31
9.4 Configure a vCloud Availability vApp Replication Manager ................................ 33
9.5 Register a vCloud Availability Replicator with a vCloud Availability Replication Manager in the Same Site ................................................................. 36
9.6 Pair Sites ........................................................................................................... 38

Replication Policy: ............................................................................................... 39
10.1 Replication Policy Conflicts ................................................................................. 41

Services Management Interface Addresses ....................................................... 43
Log Files ................................................................................................................ 43
Configuration Files ............................................................................................... 44
References ............................................................................................................. 44

List of Tables
Table 1. vCloud Availability Cloud-to-Cloud DR Component sizing .................................. 11
Table 2. vCloud Availability Cloud-to-Cloud DR Component sizing ................................ 11
Table 3. Methods Available to Protect vCloud Availability Cloud-to-Cloud DR .......... 17
Table 4. Component Counts for Highly Available vCloud Availability Cloud-to-Cloud DR Solution – Per Site ................................................................. 17
Table 5. Recommended Pre-requisite Component Counts for Highly Available vCloud Availability Cloud-to-Cloud DR Solution – Per Site ................................. 17
Table 6. Network Ports required for Local Site Communication without Tunnel Configuration ........... 23
Table 7. Network Ports required for External Site Communication without Tunnel Configuration .... 24
Table 8. Network Ports required for Local Site Communication with Tunnel Configuration ..................... 26
Table 9. Network Ports required for External Communication with Tunnel Configuration .......................... 27
Table 10. vCloud Availability Cloud-to-Cloud DR Admin Interface .............................................................................. 43
Table 11. vCloud Availability Cloud-to-Cloud DR Management Interface ................................................................. 43
Table 12. vCloud Availability Cloud-to-Cloud DR Log File .......................................................................................... 43
Table 13. vCloud Availability Cloud-to-Cloud DR Configuration Files ................................................................. 44

List of Figures

Figure 1. VMware vCloud Availability Cloud-to-Cloud Disaster Recovery Workflow .............................................. 6
Figure 2. VMware vSphere Replication Calculator ........................................................................................................ 14
Figure 3. VMware vCloud Availability Cloud-to-Cloud Disaster Recovery Conceptual Design ......................... 15
Figure 4. VMware vCloud Availability Cloud-to-Cloud Disaster Recovery Logical Design without Tunnel ..... 18
Figure 5. VMware vCloud Availability Cloud-to-Cloud Disaster Recovery Logical Design with Tunnel ....... 19
Figure 6. VMware vCloud Availability Cloud-to-Cloud DR Physical Deployment without Tunnel Appliance ......................................................................................................................... 20
Figure 7. VMware vCloud Availability Cloud-to-Cloud DR Physical Design with Tunnel Appliance ........ 21
Figure 8. Network Ports required for Local Site Communication without Tunnel Configuration .................. 22
Figure 9. Network Ports required for External Site Communication without Tunnel Configuration .......... 24
Figure 10. Network Ports required for Local Site Communication with Tunnel Configuration ................ 25
Figure 11. Network Ports required for External Communication with Tunnel Configuration .................... 27
Introduction

This guide provides information on how to architect, design and deploy vCloud Availability Cloud-to-Cloud DR solution on providers vCloud Director Powered Cloud.

1.1 Overview

The VMware Cloud Provider™ Program is an ecosystem of over 4,500 service providers located in more than 100 countries offering VMware based cloud services. Local providers protect data sovereignty while providing a wide range of cloud services and vertical market expertise through specialized compliance and certifications.

As the world’s largest network of validated cloud services based on VMware technology, the VMware Cloud Provider Program enables partners to consume VMware products on a pay-as-you-go, pay-as-you-grow, monthly subscription model. By offering a wide range of VMware-based cloud services on a geographical basis, VMware Service Provider Partners can now offer hybrid cloud services that quickly and seamlessly extend the customer’s data center into the cloud using the same VMware products and tools they already use on premise.

The VMware vCloud Availability Cloud-to-Cloud DR solution extends existing hybrid cloud offerings of VMware Cloud Providers™ on top of VMware vCloud Director with disaster recovery and application continuity between vCloud Director Virtual Data Centers or Cloud Environments. vCloud Availability Cloud-to-Cloud brings in a much-needed in providing native Disaster Recovery between vCloud Director instances. VMware vCloud Availability for Cloud-to-Cloud DR can help VMware Cloud Providers enable further monetization of existing VMware vCloud Director multi-tenant cloud environments with DR services, including replication and failover capabilities for workloads at both VM and vApp level.

1.2 vCloud Availability Cloud-to-Cloud DR Workflow

Figure 1. VMware vCloud Availability Cloud-to-Cloud Disaster Recovery Workflow
1.3 VMware vCloud Availability for Cloud-to-Cloud DR Features

VMware vCloud Availability for Cloud-to-Cloud DR Delivers below features:

- Replication and recovery of vApps (VMs) between organization Virtual Data Centers (orgVDC) as well as two instances of vCloud Director for migration, DR, and planned migration.

- The capability of each deployment to serve as both source and recovery sites. There are no dedicated source and destination sites.

- Complete self-serviceability for the provider and tenant administrator via a unified HTML5 portal that can be used alongside vCloud Director. Replication, migration, and failover can be managed completely by the tenant or provided as a managed service by the provider.

- Symmetrical replication flow that can be started from either the source or the recovery vCD instance.

- A simplified and streamlined architecture to support vCloud Director 8.20, 9.0, 9.1 and 9.5 while supporting underline vSphere 6.0, 6.5 and 6.7.

- Built-in encryption or encryption and compression of replication traffic.

- Enhanced control with white-listing of DR-enabled vCloud Director organizations, enforcement of specific min Recovery Point Objective (RPO) at an organization (org) level, maximum snapshots per org and max replications per tenant.

- Public API allowing service providers to integrate DR workflow and management into their business systems for operational automation or service usage.

- Plugins for Day 2 operational monitoring and management within vRealize Operations and plugins for vRealize Orchestrator, allowing creation and execution of DR runbooks.

- Provide Non-disruptive, on-demand disaster recovery testing.

- Policies that allow service provider administrators to control the following system attributes for one or multiple vCloud Director organizations:
  - Limit the number of replications at the vCloud Director organization level
  - Limit the minimum Recovery Point Objective (RPO)
  - Limit number of retained snapshots per VM replication
  - Limit the total number of VM replications
Use Cases

Though the most obvious use case for VMware vCloud Availability Cloud-to-Cloud DR is disaster recovery from one cloud availability zone to another cloud availability zone, it can handle a number of different use cases and provide significant capability and flexibility to service providers. For all use cases and situations, VMware vCloud Availability Cloud-to-Cloud DR supports non-disruptive testing of protected cloud workload in network and storage isolated environments. This provides the ability to test disaster recovery, disaster avoidance, or planned migrations as frequently as desired to ensure confidence in the configuration and operation of recovery on cloud. The use cases are:

2.1 Migration

A tenant or provider administrator can utilize C2C to migrate workloads from one organization VDC to another with minimal disruption from a self-service portal. End benefit is reorganizing workloads from an easy to use workflow.

- Easy to use workflow mechanism
- Organize workloads in different orgVDCs
- Ability to migrate between vCD instances or within the same vCD instance

2.2 Disaster Recovery

A service provider has multiple sites with vCD based multi-tenant environment. Customer like to do DR from one cloud provider site to another cloud site. Disaster recovery or a planned/unplanned failover is what VMware vCloud Availability Cloud-to-Cloud DR was specifically designed to accomplish for cloud providers. This helps providers and customers to achieve:

- Fastest RTO
- Recover from unexpected failure
- Full or partial site recovery

2.3 Disaster Avoidance

Preventive failover is another common use case for VMware vCloud Availability Cloud-to-Cloud DR. This can be anything from an oncoming storm to the threat of power issues.

VMware vCloud Availability Cloud-to-Cloud DR allows for the graceful shutdown of virtual machines at the protected site, full replication of data, and startup of virtual machines and applications at the recovery site ensuring app-consistency and zero data loss. Solution helps Providers and Customer in recovering from:

- Anticipate outages
- Preventive failover
- Graceful shutdown ensuring no data loss

2.4 Upgrade and Patch Testing

The VMware vCloud Availability Cloud-to-Cloud DR test environment provides a perfect location for conducting operating system and application upgrade and patch testing. Test environments are complete copies of production environments configured in an isolated network segment which ensures that testing is as realistic as possible while at the same time not impacting production workloads or replication.
vCloud Availability Cloud-to-Cloud DR Components

The architecture of VMware vCloud Availability C2C DR relies on symmetrical replication operations between cloud environments. That means there is no dedicated source and destination sites. Each site will be able to serve as both a source and a destination. VMware vCloud Availability C2C DR made up of the following components:

3.1 vSphere Replication Server and vSphere Replication Filter

The replication server receives and records delta information for each replicated virtual machine. During the cloud-to-cloud replication, delta information is sent from one ESXi host to another ESXi host.

vSphere Replication Filter intercepts VM Disk I/O and keeps tracks of which regions of virtual disk the guest is modifying and sends these updates to the remote site in a manner that results in a crash consistent replica. After configuration start with full sync of powered on VM and then Auto sync based on RPO.

Replication Server receives light weight delta from Replication Filter and writes in to the target datastore using NFC (Network File Copier). It helps in creation of failover/test images and manages retention policy.

3.2 vCloud Availability Replicator

vCloud Availability Replicator is a thin wrapper which exposes the low-level Host Based Replication primitives as REST APIs. So that HBR primitives can be consumed programmatically.

This service works as a single point for source and destination replication. This Service Talks to Replication server, Replication filter using vCenter, vCenter and LWD Proxy. It Monitors Source VM, Destination VM and vCloud Availability Replication Manager. It executes replication workflow based on the vCloud Availability Replication Manager's instructions.

3.3 vCloud Availability Replication Manager

vCloud Availability Replication Manager is a vCenter level management service. It understands the vCenter Server level concepts for starting the replication workflow for the virtual machines. Manager manages business logic, initiates workflows, orchestrates replicators and holds replication state. If any replication fails, you may start troubleshooting from here.

3.4 vCloud Availability vApp Replication Service/Manager

vCloud Availability vApp Replication Manager provides the main interface for the cloud-to-cloud replication operations. It understands the vCloud Director level concepts and works with vApps and virtual machines.

3.5 Light Weight Delta Protocol (LWD Proxy)

This service provides security like multi-tenancy, encryption and compression to the vCloud Availability Replicator. Light Weight Delta Protocol is a proprietary replication protocol ensures that each incoming replication data stream comes only from the authorized source LWD proxy instance, and each outgoing replication data stream goes only to an authorized destination LWD proxy instance.
3.6 vCloud Availability Tunnel
vCloud Availability Tunnel appliance simplifies provider networking setup by channeling all incoming and outgoing traffic for a site through a single point using the vCloud Availability Tunnel appliance.

vCloud Availability for Cloud-to-Cloud DR requires that each component on a local site has bidirectional TCP connectivity to each component on the remote site. For example, each vCloud Availability Replicator in the local site communicates with the vCloud Availability Replication Manager in the remote site (management traffic). Each vCloud Availability Replicator in the local site requires bidirectional TCP connectivity to all vCloud Availability Replicator instances in the remote site (data traffic). If authorizing all connections between sites is not a problem, you do not need to configure Cloud-to-Cloud Tunneling. If you, however, configure Cloud-to-Cloud Tunneling, you must provide connectivity between the vCloud Availability Tunnel appliances on each site. After you configure the vCloud Availability Tunnel appliances, all other traffic goes through the vCloud Availability Tunnel appliances.

3.7 vCloud Availability for Cloud-to-Cloud DR portal

The vCloud Availability for Cloud-to-Cloud DR portal provides tenants and service providers with a graphic user interface to facilitate the management of the vCloud Availability for Cloud-to-Cloud DR solution. The vCloud Availability for Cloud-to-Cloud DR portal also provides overall system and workload information.
vCloud Availability Cloud-to-Cloud DR Node Types and Sizing

Installation of all vCloud Availability for Cloud-to-Cloud DR services by using a single installation OVA package. Use the same OVA package to deploy vCloud Availability for Cloud-to-Cloud DR appliances in all your cloud sites. The Service Provider’s environment will consist of multiple components that operate together to provide replication, secure communications, and storage of the replicated data. The components that reside in the Service Provider environment are described in the following table.

4.1 Node Deployment Types (Service Provider Components):

The following table describes the different node types:

Table 1. vCloud Availability Cloud-to-Cloud DR Component sizing

<table>
<thead>
<tr>
<th>Node Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Combined  | All-in-one deployment type that is suitable for testing, evaluation, and small deployments. Includes the following roles:  
- vCloud Availability Replication Manager  
- vCloud Availability Replicator  
- vCloud Availability vApp Replication Manager  
- vCloud Availability for Cloud-to-Cloud DR Portal |
| Manager Node | Used for a deployment of a dedicated vCloud Availability Replication Manager appliance. |
| Manager Node with vCloud Director support | Used for a deployment of a single appliance that contains the following services:  
- vCloud Availability Replication Manager  
- vCloud Availability vApp Replication Manager  
- vCloud Availability for Cloud-to-Cloud DR Portal |
| Replicator Node | This node will be used for a deployment of a dedicated vCloud Availability Replicator appliance which hosts vSphere Replication Server, vSphere Replication Filter, vCloud Availability Replicator and Light Weight Delta protocol (LWD Proxy) |
| Large Replicator Node | This node will be used for a deployment of a dedicated vCloud Availability Replicator appliance which hosts vSphere Replication Server, vSphere Replication Filter, vCloud Availability Replicator and Light Weight Delta protocol (LWD Proxy) |
| Tunnel Node | Used for a deployment of a vCloud Availability Tunnel appliance. |

4.2 Node Sizing:

The following table describes the different node deployment sizing.

Table 2. vCloud Availability Cloud-to-Cloud DR Component sizing

<table>
<thead>
<tr>
<th>Node Type</th>
<th>vCPU</th>
<th>Memory</th>
<th>Disk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combined</td>
<td>4</td>
<td>6 GB</td>
<td>10 GB</td>
</tr>
<tr>
<td>Manager Node with vCD Support</td>
<td>4</td>
<td>4 GB</td>
<td>10 GB</td>
</tr>
</tbody>
</table>
4.3 vCloud Availability Cloud-to-Cloud DR Operational Limits:

Following operational guidelines apply to vCloud Availability Cloud-to-Cloud DR 1.5:

- A single Tenant can have 300 Active protections.
- A Single Large Replicator appliance supports 300 Active protection.
- 3000 Active Protection across 100 tenants.
- 100 tenants can run with active replications.
- Provider can have 7 Active Replicator instances.
- Up to 120 concurrent Protect, Test Failover, Failover and Reverse Protect operations.
- 65 Concurrent Failover operations.
- vCloud Availability Cloud-to-Cloud DR does not support Datastore Clusters as a replication destination.
- It also does not support reverse operations for which a datastore cluster has been used as a source.

vCloud Availability Cloud-to-Cloud DR Deployment Requirements

Before you start deploying and configuring vCloud Availability for Cloud-to-Cloud DR services, ensure that provider environment meets the following requirements:

5.1 VMware vCloud Director and SSO

VMware vCloud Availability Cloud-to-Cloud DR solution require two sites and each site should have highly Available, production grade vCloud Director deployed with:

- A shared Management Cluster containing the vCloud Director Cells, vCloud Director database, and the other core components and services needed to run the cloud.
- One or more resource groups representing dedicated resources for cloud consumption. Each resource group is a number of clusters of ESXi hosts managed by a vCenter Server and is under the control of vCloud Director. Multiple resource groups can be managed by the same vCloud Director instance.
- The resource vCenter Server within a vCloud Director site must be within the same SSO domain. Therefore, one must utilize a single SSO domain for vCD/management and resource clusters.
- All vCloud Availability Replicator appliances within the respective site must be configured with that same SSO domain.

5.2 Network Requirements

- The vCloud Availability vApp Replication Service/Manager must have TCP access to vCloud Director, vCloud Availability Replication Manager, vCenter Server or PSC in local site.
- The vCloud Availability Replication Manager must have TCP access to the Lookup Service and all the vCloud Availability Replicator appliances in both local and remote sites.
5.3 Replication and Network Bandwidth Requirements

The business requirements and potential revenue impact for each application must be compared to the cost of a replication technology solution.

The main replication technologies are as follows:

- **Synchronous replication** – Every write on the protected site must be acknowledged by the recovery site before the protected site can acknowledge the write. An RPO of zero can be achieved, but distances are limited by bandwidth and latency. The theoretical maximum distance with less than 5 ms of round-trip latency is 465.7 miles. However, in practice, synchronous replication cannot be used over a distance of about 100 km (Approx. 60 miles).

- **Asynchronous replication** – Asynchronous replication goes much further, but data is sent to the recovery site with some lag time. RPO is affected, and data loss depends on technology, bandwidth, I/O load on production, and cycle time (repetitive cycle comparing the changes made during a predefined time period).

- **Continuous replication** – Journaled replication is similar to asynchronous replication. However, the changes are journaled. Therefore, multiple recovery points are available. The most recent recovery point is still a function of technology, bandwidth, and I/O load.

Storage and Network bandwidth requirements can increase when using VMware vCloud Availability Cloud-to-Cloud DR. The following factors play a major role in the amount of network bandwidth vCloud Availability Cloud-to-Cloud DR requires for efficient replication.

5.3.1 Network Based Storage

Network bandwidth requirements within data center increase if all storage is network-based because data operations between the host and the storage also use network. When you plan your deployment, be aware of the following levels of traffic:

- Between the host running the replicated virtual machine and the vCloud Availability Cloud-to-Cloud DR Replicator.
- Between the vCloud Availability Cloud-to-Cloud DR Replicator and a host with access to the replication target datastore.
- Between the ESXi host and Network Storage.

When you have two sites the link speed between the two sites is the most important as it can slow down replication traffic between the two sites.

5.3.2 Data Change Rate and Recovery Point Objective

The data change rate is affected by the recovery point objective (RPO). To estimate the size of the data transfer for each replication, you must evaluate how many blocks change in a given RPO for a virtual machine. The data change rate within the RPO period provides the total number of blocks that Replicator transfers. This number might vary throughout the day, which alters the traffic that replicator generates at different times.
Replicator transfers blocks based on the RPO policy. If you set an RPO of one hour, Solution transfers any block that has changed in that hour to meet that RPO. Replicator only registers that the block has changed within the RPO period, not how many times it changed. The average daily data change rate provides an estimation of how much data replicator transfers or how often the transfers occur.

If you use volume shadow copy service (VSS) to quiesce the virtual machine, replication traffic cannot be spread out in small sets of bundles throughout the RPO period. Instead, replicator transfers all the changed blocks as one set when the virtual machine is idle. Without VSS, replicator can transfer smaller bundles of changed blocks on an ongoing basis as the blocks change, spreading the traffic throughout the RPO period. The traffic changes if you use VSS and replicator handles the replication schedule differently, leading to varying traffic patterns.

The compliance of RPO depends on the ability to transfer workload changed data from the protected site to the recovery site in a given (RTO) time. The data transfer is constrained by the network bandwidth available between the sites. Considerations must be given to have wide enough pipe between sites. The replication bandwidth requirements mostly depend on the following factors:

- Number of protected VMs
- Average disk size
- Average utilization
- Average rate of change
- RPO
- Enabled compression

5.3.3 Bandwidth Calculation


**Figure 2. VMware vSphere Replication Calculator**
Or follow this KB - [https://kb.vmware.com/s/article/2037268](https://kb.vmware.com/s/article/2037268) for more information on Bandwidth calculations.

### 5.3.4 Other Configuration Change requirements:

- Disable vCloud Director Discovery virtual machine feature else might face issues with failover and test operations.
- The vCloud Availability for Cloud-to-Cloud DR services perform a host name certificate verification. Therefore, it is expected that the Common Name or at least one of the entries in the Subject Alternative Name of the vCloud Director certificate matches the vCloud Director address (FQDN or IP) that is used during vCloud Director registration.

## vCloud Availability Cloud-to-Cloud DR Architecture Design

### 6.1 vCloud Availability Cloud-to-Cloud DR Conceptual Design

This conceptual design is meant to be a high-level overview of the design of vCloud Availability Cloud-to-Cloud DR.

**Figure 3. VMware vCloud Availability Cloud-to-Cloud Disaster Recovery Conceptual Design**

[Diagram showing the conceptual design of vCloud Availability for Cloud-to-Cloud DR, with two zones labeled DC-Zone-A and DC-Zone-B, each containing Disaster Recovery Recovery Site, Replicated VMs, Protected VMs, and VMware Powered Cloud.]
6.2 vCloud Availability Cloud-to-Cloud DR Logical Design

This VMware vCloud Availability Cloud-to-Cloud DR design includes a total of two Cloud Sites. Both the sites have been deployed with VMware SDDC with vCloud Director Based Cloud. Each Site provides specific functions as follows:

- **Cloud Site-A** – This Cloud data center is having VMware SDDC deployed and on top of SDDC vCloud Director Based Cloud has been deployed and serve many customers of zone A.

- **Cloud Site-B** – This Cloud data center is having VMware SDDC deployed and on top of SDDC vCloud Director Based Cloud has been deployed and serve many customers of zone B.

Zone A customer will have their workload deployed in Site-A of Zone-A and looking to have Disaster recovery solution on the cloud in different zone, Site-B of Zone B of the provider will be considered as DR site

Zone B customer will have their workload deployed in Site-B of Zone-B and looking to have Disaster recovery solution on the cloud in different zone, Site-A of Zone A of the provider will be considered as DR site

The following represents the overall logical design for the Cloud-to-Cloud disaster recovery solution for service providers. Customer has various business applications and services, that must remain available, even in the event of a disaster. There is network connectivity between Site-A and Site-B, and data from Site-A is replicated to Site-B and vice versa using vCloud Availability Replication.

6.3 Servers for vCloud Availability Cloud-to-Cloud DR without Tunnel Appliance

A Manager Node with vCD Support and Replicator Node is required at both the primary site (can be referred as the protected site or recovery site) and the secondary site (can be referred as the recovery site or protected site). The vCloud Availability Cloud-to-Cloud DR operates as an extension to the vCloud Director at a site. Because the vCloud Availability Cloud-to-Cloud DR server depends on vCloud Director, vCenter Server and VMware Platform Services Controller for some services, you must install and configure vCloud Director, vCenter Server and Platform Services Controller at a site before vCloud Availability Cloud-to-Cloud DR can be implemented.

6.3.1 Manager Node with vCD Support - Consider deploying a single appliance of Manager Node with vCD Support using vCloud Availability ova. High Availability of the node will be based on vSphere HA.

6.3.2 Replicator Node - Consider deploying two Replicator Appliance using vCloud Availability OVA. Register both the appliances with Manager node, so in case one Replicator appliance fails, job can be transferred to another replicator appliance.

6.4 Servers for vCloud Availability Cloud-to-Cloud DR with Tunnel Appliance

A Manager Node with vCD Support and Replicator Node is required at both the primary site (can be referred as the protected site or recovery site) and the secondary site (can be referred as the recovery site or protected site). The vCloud Availability Cloud-to-Cloud DR operates as an extension to the vCloud Director at a site. Because the vCloud Availability Cloud-to-Cloud DR server depends on vCloud Director, vCenter Server and VMware Platform Services Controller for some services, you must install and configure vCloud Director, vCenter Server and Platform Services Controller at a site before vCloud Availability Cloud-to-Cloud DR can be implemented.
6.4.1 Manager Node with vCD Support - Consider deploying a single appliance of Manager Node with vCD Support using vCloud Availability ova. High Availability of the node will be based on vSphere HA.

6.4.2 Replicator Node - Consider deploying two Replicator Appliance using vCloud Availability OVA. Register both the appliances with Manager node, so in case one Replicator appliance fails, job can be transferred to another replicator appliance.

6.4.3 vCloud Availability Tunnel node – By default vCloud Availability Cloud-to-Cloud DR solution requires by-directional TCP connectivity across provider data centers. and if providers are having problem having by-direction connectivity across data centers, then configure Cloud-to-Cloud Tunneling. Tunnel appliance works as a single point for entry and exit point for replication and management. Both the tunnel appliance can be connected to the internet/wan connectivity to establish the connectivity.

6.5 High Availability for vCloud Availability Cloud-to-Cloud DR
Availability of vCloud Availability Cloud-to-Cloud DR is critical due to the ability to manage the environment, replication and RPO compliance at all times. To avoid extended periods of downtime, use a highly available configuration.

Table 3. Methods Available to Protect vCloud Availability Cloud-to-Cloud DR

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated protection using vSphere HA.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Deploy Multiple appliances with Native HA</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

6.6 Minimum High Availability Component for vCloud Availability Cloud-to-Cloud DR
To sustain a highly available vCloud Availability Cloud-to-Cloud DR solution, consider the following counts per component.

Table 4. Component Counts for Highly Available vCloud Availability Cloud-to-Cloud DR Solution – Per Site

<table>
<thead>
<tr>
<th>Component</th>
<th>Number of Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability Replicator or Large Replicator</td>
<td>2</td>
</tr>
<tr>
<td>Manager node with vCloud Director support</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 5. Recommended Pre-requisite Component Counts for Highly Available vCloud Availability Cloud-to-Cloud DR Solution – Per Site

<table>
<thead>
<tr>
<th>Component</th>
<th>Number of Instances</th>
</tr>
</thead>
</table>
### vCloud Availability Cloud-to-Cloud DR

<table>
<thead>
<tr>
<th>Component</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Director</td>
<td>2</td>
</tr>
<tr>
<td>vCenter Server (1 Management, 1 Resource)</td>
<td></td>
</tr>
<tr>
<td>External Platform Services Controller (PSC)</td>
<td>2 with HA</td>
</tr>
<tr>
<td>vCloud Availability Replicator</td>
<td>2</td>
</tr>
<tr>
<td>Manager node with vCloud Director support</td>
<td>1</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>1</td>
</tr>
<tr>
<td>vCD Supported Database</td>
<td>1</td>
</tr>
<tr>
<td>NFS/NFS Server</td>
<td>1</td>
</tr>
<tr>
<td>Cassandra Host</td>
<td>3</td>
</tr>
<tr>
<td>RabbitMQ Host</td>
<td>2</td>
</tr>
</tbody>
</table>

**Figure 4. VMware vCloud Availability Cloud-to-Cloud Disaster Recovery Logical Design without Tunnel**
Figure 5. VMware vCloud Availability Cloud-to-Cloud Disaster Recovery Logical Design with Tunnel
Physical Design

As of vCloud Availability Cloud-to-Cloud DR 1.5, installation and configuration has been dramatically simplified. The vCloud Availability Cloud-to-Cloud DR specifications should be able to accommodate all the necessary services that are being used. This section describes different aspects of the physical design of vCloud Availability Cloud-to-Cloud DR configuration for the Cloud-to-Cloud DR Implementation.

7.1 vCloud Availability Cloud-to-Cloud DR Sites and Locations

The vCloud Availability Cloud-to-Cloud DR infrastructure will be deployed at two sites. Within each site, there will be two vCloud Availability Replicator node and one vCloud Availability Cloud-to-Cloud DR Manager.

7.2 vCloud Availability Cloud-to-Cloud DR deployment without tunnel appliance

vCloud Availability for Cloud-to-Cloud DR requires that each component on a local site has bidirectional TCP connectivity to each component on the remote site. For example, each vCloud Availability Replicator in the local site communicates with the vCloud Availability Replication Manager in the remote site for management traffic. Similarly, each vCloud Availability Replicator in the local site requires bidirectional TCP connectivity to all vCloud Availability Replicator instances in the remote site for data traffic. If bidirectional TCP connectivity across your data centers are not a problem, then this is the preferred method of the deployment.

Figure 6. VMware vCloud Availability Cloud-to-Cloud DR Physical Deployment without Tunnel Appliance
7.3 vCloud Availability Cloud-to-Cloud DR deployment with tunnel appliance.

If by-directional TCP connectivity across provider data centers are problem, then configure Cloud-to-Cloud Tunneling. You must provide connectivity between the vCloud Availability Tunnel appliances on each site. After you configure the vCloud Availability Tunnel appliances, all cross-site traffic goes through the vCloud Availability Tunnel appliances.

**Figure 7. VMware vCloud Availability Cloud-to-Cloud DR Physical Design with Tunnel Appliance**

7.4 Replace vCloud Availability vApp Replication Manager Certificate with a CA Signed Certificate

To configure the vCloud Availability vApp Replication Manager to work with a CA-signed certificate. Make sure that you have the third-party signed certificate and its corresponding private key in a P12-formatted file. Follow below documented procedure for replacement of certificate.

Network Communication and Firewalls

To ensure vCloud Availability for Cloud-to-Cloud DR services can communicate within a single site and between source and destination sites, ensure that the required network ports are opened. The network port configuration is different for deployments with and without a Cloud-to-Cloud Tunneling.

8.1 Network Ports for Local Site Connection Without Cloud-to-Cloud Tunneling

The communications port settings for vCloud Availability Cloud-to-Cloud DR, see the table following the figure:

Figure 8. Network Ports required for Local Site Communication without Tunnel Configuration
### Table 6. Network Ports required for Local Site Communication without Tunnel Configuration

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port Number</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability Replicator service</td>
<td>Local ESXi hosts</td>
<td>80</td>
<td>HTTPS</td>
<td>Used to establish a connection between local vCloud Availability Replicator service and local ESXi hosts before initial replication starts.</td>
</tr>
<tr>
<td>vCloud Availability for Cloud-to-Cloud DR services that use single sign-on.</td>
<td>All Platform Services Controllers (PSC) in the same single sign-on domain. Used only if external PSC is used.</td>
<td>443</td>
<td>HTTPS</td>
<td>Used by vCloud Availability for Cloud-to-Cloud DR services for single sign-on and Lookup Service communication when vSphere 6.0 or later is used in the respective site.</td>
</tr>
<tr>
<td>vCloud Availability vApp Replication Service/Manager service or vCloud Availability Replicator service</td>
<td>All PSCs</td>
<td>7444</td>
<td>TCP</td>
<td>Used for single sign-on and Lookup Service communication when vSphere 5.5 or later is used in the respective site.</td>
</tr>
<tr>
<td>vCloud Availability vApp Replication Service/Manager service or vCloud Availability Replicator Service</td>
<td>Local vCenter Server</td>
<td>443</td>
<td>HTTPS</td>
<td>Used by the local vCloud Availability vApp Replication Service/Manager service or the vCloud Availability Replicator service for communication with the local vCenter Server.</td>
</tr>
<tr>
<td>vCloud Availability Replicator service</td>
<td>Local ESXi hosts</td>
<td>902</td>
<td>TCP and UDP</td>
<td>Used by the vCloud Availability Replicator service for replication traffic to the destination ESXi hosts.</td>
</tr>
<tr>
<td>Local ESXi hosts</td>
<td>Local LWD Proxy service</td>
<td>44046</td>
<td>LWD</td>
<td>Used for replication data traffic from a protected ESXi host to the local LWD Proxy.</td>
</tr>
</tbody>
</table>
8.2 Network Ports for External Communication Without Cloud-to-Cloud Tunneling

The communications port settings for vCloud Availability Cloud-to-Cloud DR, see the table following the figure:

**Figure 9. Network Ports required for External Site Communication without Tunnel Configuration**

<table>
<thead>
<tr>
<th>Source/Service</th>
<th>Destination/Service</th>
<th>Port Number</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source LWD Proxy</td>
<td>Local LWD Proxy</td>
<td>44045</td>
<td>LWDS</td>
<td>Used for replication data traffic from a source site to all local vCloud Availability Replicator instances.</td>
</tr>
<tr>
<td>End-user Web browser</td>
<td>vCloud Availability vApp Replication Service/Manager service</td>
<td>8443</td>
<td>HTTPS</td>
<td>The vCloud Availability vApp Replication Service/Manager user interface that is exposed to the end user.</td>
</tr>
<tr>
<td>System administrator Web browser</td>
<td>Local vCloud Availability for Cloud-to-Cloud DR appliances</td>
<td>443</td>
<td>HTTPS</td>
<td>Management user interface of each appliance used for configuring vCloud Availability for Cloud-to-Cloud DR services.</td>
</tr>
<tr>
<td>vCloud Availability vApp Replication Service/Manager service in the source site</td>
<td>vCloud Availability vApp Replication Service/Manager service in the destination site</td>
<td>8046</td>
<td>HTTPS</td>
<td>Used for vCloud Availability vApp Replication Service/Manager management from a source site to a local vCloud Availability vApp Replication Service/Manager service.</td>
</tr>
<tr>
<td>vCloud Availability Replication Manager service in the source site</td>
<td>vCloud Availability Replicator service in the destination site</td>
<td>8043</td>
<td>HTTPS</td>
<td>Used for vCloud Availability Replicator management from a source site to vCloud Availability Replication Manager service.</td>
</tr>
<tr>
<td>vCloud Availability Replicator service in the source site</td>
<td>vCloud Availability Replication Manager service instances in the destination site</td>
<td>8044</td>
<td>HTTPS</td>
<td>Used for communication between the vCloud Availability Replicator instances in the source site and the vCloud Availability Replication Manager instances in the remote site.</td>
</tr>
</tbody>
</table>
8.3 Network Ports for Internal Communication with Cloud-to-Cloud Tunneling

The communications port settings for vCloud Availability Cloud-to-Cloud DR Internal communication with Tunneling appliance, see the table following the figure:

**Figure 10. Network Ports required for Local Site Communication with Tunnel Configuration**
Table 8. Network Ports required for Local Site Communication with Tunnel Configuration

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port Number</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability Replicator service</td>
<td>Local ESXi hosts</td>
<td>80</td>
<td>HTTPS</td>
<td>Used to establish a connection between local vCloud Availability Replicator service and local ESXi hosts before initial replication starts.</td>
</tr>
<tr>
<td>vCloud Availability for Cloud-to-Cloud DR services that use single sign-on.</td>
<td>All Platform Services Controllers (PSC) in the same single sign-on domain. Used only if external PSC is used.</td>
<td>443</td>
<td>HTTPS</td>
<td>Used by vCloud Availability for Cloud-to-Cloud DR services for single sign-on and Lookup Service communication when vSphere 6.0 or later is used in the respective site.</td>
</tr>
<tr>
<td>vCloud Availability vApp Replication Service/Manager service or vCloud Availability Replicator service</td>
<td>All PSCs</td>
<td>7444</td>
<td>TCP</td>
<td>Used for single sign-on and Lookup Service communication when vSphere 5.5 or later is used in the respective site.</td>
</tr>
<tr>
<td>vCloud Availability vApp Replication Service/Manager service or vCloud Availability Replicator Service</td>
<td>Local vCenter Server</td>
<td>443</td>
<td>HTTPS</td>
<td>Used by the local vCloud Availability vApp Replication Service/Manager service or the vCloud Availability Replicator service for communication with the local vCenter Server.</td>
</tr>
<tr>
<td>vCloud Availability Replicator service</td>
<td>Local ESXi hosts</td>
<td>902</td>
<td>TCP and UDP</td>
<td>Used by the vCloud Availability Replicator service for replication traffic to the destination ESXi hosts.</td>
</tr>
<tr>
<td>Local ESXi hosts</td>
<td>Local LWD Proxy service</td>
<td>44046</td>
<td>LWD</td>
<td>Used for replication data traffic from a protected ESXi host to the local LWD Proxy.</td>
</tr>
<tr>
<td>vCloud Availability Tunnel appliance</td>
<td>Local LWD Proxy service</td>
<td>44045</td>
<td>LWDS</td>
<td>Used for replication data traffic from the vCloud Availability Tunnel to all local vCloud Availability Replicator instances.</td>
</tr>
<tr>
<td>vCloud Availability Tunnel appliance</td>
<td>vCloud Availability vApp Replication Manager service</td>
<td>8046</td>
<td>HTTPS</td>
<td>vCloud Availability vApp Replication Manager service management from the vCloud Availability Tunnel appliance.</td>
</tr>
<tr>
<td>vCloud Availability Tunnel appliance</td>
<td>vCloud Availability Replicator service</td>
<td>8043</td>
<td>HTTPS</td>
<td>vCloud Availability Replicator management from the vCloud Availability Tunnel.</td>
</tr>
<tr>
<td>vCloud Availability Tunnel appliance</td>
<td>vCloud Availability Replication Manager</td>
<td>8044</td>
<td>HTTPS</td>
<td>Used for management traffic from the vCloud Availability Tunnel to the vCloud Availability Replication Manager within a site.</td>
</tr>
</tbody>
</table>
8.4 Network Ports for External Communication with Cloud-to-Cloud Tunneling

The communications port settings for vCloud Availability Cloud-to-Cloud DR Internal communication with Tunneling appliance, see the table following the figure:

Figure 11. Network Ports required for External Communication with Tunnel Configuration

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port Number</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Network</td>
<td>vCloud Availability Tunnel appliance</td>
<td>8048</td>
<td>Any</td>
<td>Replication management and data traffic from a source site to the local vCloud Availability Tunnel appliance.</td>
</tr>
</tbody>
</table>
Deployment

First step in deployment and configuration of vCloud Availability Cloud-to-Cloud DR is to deploy the vCloud Availability Cloud-to-Cloud DR appliances. In this guide a set of appliances will be deployed across two vCD cloud sites. vCloud Availability Cloud-to-Cloud DR comes in a single ovf file, which can be deployed as a combined deployment that includes all components into a single appliance, or role based deployment with multiple appliances running different services.

Since All-in-one deployment option is only intended for POC type of deployment, we won't be leveraging it for any production deployments. Instead, we will leverage the scale out deployment option, which deploys one Manager node and one or more Large Replicator nodes. Each vCloud Availability Cloud-to-Cloud DR instance will initially be deployed with a single Manager and a Single Large Replicator node and based on the needs additional Large replicator nodes will be added based on demand.

9.1 Deploy vCloud Availability Cloud-to-Cloud DR OVA

Follow these Steps for each Sites

The deployment of vCloud Availability Cloud-to-Cloud DR OVA is like any other OVA/OVF deployment. The only important part in deploying the appliance is selecting the role it is going to perform, in this case we will be deploying :

- Manager Node with vCloud Director Support
- Large Replicator Node
Using standard procedure of OVA deployment method deploy three appliances one for management components and two for replication.

Once you have deployed three appliances, one Manager with vCD support , and two Replicators then follow the below process to integrate them together.

- Configure a vCloud Availability Replication Manager – https://appliance-ip-address:8044
- Configure a vCloud Availability vApp Replication Manager – https://appliance-ip-address/ui/admin
- Register a vCloud Availability Replicator with a vCloud Availability Replication Manager – https://appliance-ip-address:8044

9.2 Configure vCloud Availability Cloud-to-Cloud DR Replicator

First step in the configuration process is to configure the vCloud Availability Cloud-to-Cloud DR Replicator Service. This service lives on the Replicator Node that was deployed in previous steps. To configure a vCAV Replicator register the vCloud Availability Replicator appliance to a Lookup service follow below steps to configure:

Browse and login to https://Appliance-IP-address:8043

Note you will need to change the password once logging into the Replicator for the first time.

Enter a valid Lookup service address and click APPLY. Lookup service address in the following format https://Appliance-IP-address:port-number/lookupservice/sdk
Lookup Service Details

Enter connection details for the Lookup Service.

Lookup service address *  
https://vcsa-01b.corp.local/lookupservice/sdk

Accept Certificate

vCloud Availability Cloud-to-Cloud DR Portal

System health

- Instance ID: 82354ef1-0d1b-4201-93f6-0cbf78695c1
- Server time: 10/2/2018, 2:56 AM
- Lookup Service connectivity: OK
- Database connectivity: OK
- LWD connectivity: OK
- VRS connectivity: OK
9.3 Configure a vCloud Availability Replication Manager

vCloud Availability Replication manager service which runs on the Manager Node

Login using Web browser and go to https://Appliance-IP-address:8044

Log in with the appliance root password. You will be redirected to the System Monitoring tab. Navigate to the Configuration tab and in the Lookup service address area click Edit.

Enter a valid Lookup service address and click APPLY. Lookup service address in the following format https://Appliance-IP-address:port-number/lookupservice/sdk.
Review the lookup service certificate details and click Accept.
9.4 Configure a vCloud Availability vApp Replication Manager

To configure a vCloud Availability vApp Replication Manager service, enter a site name and this site name will be used as identifier and register the vCloud Availability vApp Replication Manager to a Lookup service. Then set up the vCloud Availability Replication Manager and the vCloud Director integration.

In a Web browser, go to https://Appliance-IP-address/ui/admin which opens the vCloud Availability vApp Replication Manager service management interface login page

- Log in with the appliance root password. You are redirected to the Getting Started tab.
- Click on “Run initial setup wizard”

Enter a Site Name and optionally enter a Site Description and click Next.

NOTE - Site name that you enter, as it is used as an identifier and cannot be changed later
Enter lookup service address, an single sign-on user name and password, and click Next.

Lookup service address format - `https://Lookup-Service-IP-address:443/lookupservice/sdk`.

Review the lookup service certificate details and click Accept, next Set up integration with vCloud Director. Select the appropriate Configuration Type.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover the vCloud Director service address automatically</td>
<td>By default, the option is selected. Leave the default option, if vCloud Director is federated with a previously specified lookup service, there is only one registered vCloud Director in the lookup service and the single sign-on user belongs to the System administrator group in vCloud Director.</td>
</tr>
<tr>
<td>Enter details for the vCloud Director Service manually</td>
<td>Select this option, if your vCloud Director instance is not federated with a previously specified lookup service.</td>
</tr>
</tbody>
</table>
Enter a valid vCloud Availability for Cloud-to-Cloud DR license key

Review the vCloud Availability vApp Replication Manager configuration summary and click Finish.
9.5 Register a vCloud Availability Replicator with a vCloud Availability Replication Manager in the Same Site

You need to register a vCloud Availability Replicator to a vCloud Availability Replication Manager in the same site, so that the two services can work together. Site-A Replicator will be registered with Site-A Replication Manager and Site-B Replication will be registered with Site-B Replication Manager.

In a Web browser, go to https://Manager-IP-address:8044/admin. The vCloud Availability Replication Manager service management interface login page opens.

Log in with the appliance root password that you set during the initial vCloud Availability Replicator configuration. In the Replicators tab, click New.
Enter the details as described in the figure below:

In this example, I have configured two Replicator for High Availability.

This completes procedure for the deployment and integration of vCloud Availability Cloud-to-Cloud DR components.
9.6 Pair Sites

Once installation and integration of vCloud Availability Cloud-to-Cloud DR component is completed, we need to establish trust between vCloud Availability vApp Replication Service/Manager instances in which got deployed across two different sites. You can initiate a cloud sites pairing from either one of the sites that you want to establish a trust between.

In a Web Browser, go to the vCloud Availability vApp Replication Service/Manager Configuration Portal at https://Appliance-IP-Address:8046. Go to Cloud SITES > NEW CLOUD SITE.
Click on “PAIR”, Accept Certificate, to Verify the trust , go to Cloud Sites and confirm that new site is listed without errors and warnings.

Above steps complete the Pairing process of the sites. But before you can configure replications of VM and vApps, you must create a replication policy and assign it to the source and destination vCloud Director organizations. The replication policy that is assigned to the source and destination organizations must allow replications.

**Replication Policy:**

Replication policies control replication attributes of vCloud Director organization from the vCloud Availability for Cloud-to-Cloud DR solution perspective. By creating and assigning a replication policy to an organization, you can enable or disable the organization for incoming or outgoing replications. You control the minimum Recovery Point Objective (RPO) value that tenants can set and can set a maximum number of virtual machine replications and retained snapshots per replication that are permitted for tenant users. You create, edit, assign, and delete replication policies from the Policies tab.

**NOTE** - One replication policy can be assigned to multiple vCloud Director organizations. There is one editable, **default replication policy** that you cannot delete. All organizations that are not associated with a custom replication policy, are assigned to the default policy, which is set with below configurations:

- Outgoing replications are not allowed.
- Incoming replications are not allowed.
- Minimum RPO is set to 15 minutes.
- Maximum number retained snapshots per VM replication are set to 24.
- Maximum number of VM replications is set to 0.
You can create, edit, assign, and delete replication policies from the Policies tab. Log in to the vCloud Availability for Cloud-to-Cloud DR portal using System administrator credentials and click Policies.

Click New to create a new policy: Replication policies enforce the following replication attributes for an organization from the service provider prospective:

- Can an organization be used as a replication source.
- Can an organization be used as a replication destination.
- What is the Minimum Recovery Point Objective (RPO) for an organization?
- Maximum number of retained snapshots per single virtual machine replication within an organization.
- Maximum number of VM replications that can be created within an organization.

Once the replication policy is created, this appears in the replication policies list on the Policies tab of the vCloud Availability for Cloud-to-Cloud DR portal. You can assign the new policy to a vCloud Director organization.
The policy is assigned to the vCloud Director organization that you select. When you select the same policy, a list of all organizations to which the policy is assigned appears. If there are conflicts between the assigned replication policy and the existing replications, you must resolve the conflicts manually.

### 10.1 Replication Policy Conflicts

Assigning a policy to an organization or modifying existing policy for an organization can result in conflicts. E.g. - to increase the minimum allowed RPO setting for an organization, you modify the existing replication policy, or assign a new one. After the modification, all new replications within the organization must adhere to the new setting, but existing replications are not affected by the change. Existing VM will continue to use existing replication policy.

To check for replication policy conflicts, use the Compliance status table in the vCloud Availability for Cloud-to-Cloud DR portal. The Compliance status table lists all vCloud Director organizations to which a selected policy is assigned and if there are any replication policy conflicts. If there are conflicts, you must manually find the replications that cause the policy conflict.

You resolve a replication policy conflicts manually by modifying the replication settings of all replications that violate the new or modified policy, or by editing the policy settings.

To resolve a replication policy conflict, reconfigure or stop the violating replication. You can also, pause, migrate, or failover the violating replications, or edit the replication policy that the replications are violating.
### vCloud Availability Cloud-to-Cloud DR

<table>
<thead>
<tr>
<th>Name</th>
<th>Outgoing Replications</th>
<th>Ingressing Replications</th>
<th>Minimum BPO</th>
<th>Maximum Ingressing Replications</th>
<th>Maximum Snapshots</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="Org1">Org1</a></td>
<td>Allowed</td>
<td>Allowed</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>[Default Policy (default)] (Org1)</td>
<td>Allowed</td>
<td>Allowed</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Services Management Interface Addresses

The vCloud Availability for C2C DR services provides a management interface for configuration and administration. The following table can help you understand how to access the admin interface of each service.

Table 10. vCloud Availability Cloud-to-Cloud DR Admin Interface

<table>
<thead>
<tr>
<th>vCloud Availability for Cloud-to-Cloud DR Component</th>
<th>Admin Interface Address and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability vApp Replication Manager</td>
<td>https://&lt;host&gt;:8046/ui/admin</td>
</tr>
<tr>
<td>vCloud Availability Replication Manager</td>
<td>https://&lt;host&gt;:8044/ui/admin</td>
</tr>
<tr>
<td>vCloud Availability Replicator</td>
<td>https://&lt;host&gt;:8043/ui/admin</td>
</tr>
<tr>
<td>vCloud Availability Tunnel</td>
<td>https://&lt;host&gt;:8047/ui/admin</td>
</tr>
</tbody>
</table>

The following table can help you understand how to access the management interface of each service.

Table 11. vCloud Availability Cloud-to-Cloud DR Management Interface

<table>
<thead>
<tr>
<th>vCloud Availability for Cloud-to-Cloud DR Component</th>
<th>Management Interface Address and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability Replication Manager</td>
<td>https://&lt;host&gt;:8044</td>
</tr>
<tr>
<td>vCloud Availability Replicator</td>
<td>https://&lt;host&gt;:8043</td>
</tr>
<tr>
<td>vCloud Availability vApp Replication Manager</td>
<td>https://&lt;host&gt;:8046</td>
</tr>
<tr>
<td>vCloud Availability Tunnel</td>
<td>https://&lt;host&gt;:8047</td>
</tr>
<tr>
<td>vCloud Availability for Cloud-to-Cloud DR portal</td>
<td>https://&lt;host&gt;/ui</td>
</tr>
</tbody>
</table>

Log Files

Table 12. vCloud Availability Cloud-to-Cloud DR Log File

<table>
<thead>
<tr>
<th>Service</th>
<th>Default Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability Replication Manager</td>
<td>/opt/vmware/h4/manager/log/manager.log</td>
</tr>
<tr>
<td>vCloud Availability Replicator</td>
<td>/opt/vmware/h4/replicator/log/replicator.log</td>
</tr>
<tr>
<td>vCloud Availability vApp Replication Manager</td>
<td>/opt/vmware/h4/cloud/log/cloud.log</td>
</tr>
<tr>
<td>vCloud Availability Tunnel</td>
<td>/opt/vmware/h4/tunnel/log/tunnel.log</td>
</tr>
</tbody>
</table>
Configuration Files

Table 13. vCloud Availability Cloud-to-Cloud DR Configuration Files

<table>
<thead>
<tr>
<th>Service</th>
<th>Default Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Availability Replication Manager</td>
<td>/opt/vmware/h4/manager/config/application.properties</td>
</tr>
<tr>
<td>vCloud Availability Replicator</td>
<td>/opt/vmware/h4/replicator/config/application.properties</td>
</tr>
<tr>
<td>vCloud Availability vApp Replication Manager</td>
<td>/opt/vmware/h4/cloud/config/application.properties</td>
</tr>
<tr>
<td>vCloud Availability Tunnel</td>
<td>/opt/vmware/h4/tunnel/config/application.properties</td>
</tr>
</tbody>
</table>

References

Additional information pertinent to this document and its topics:

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Link or URL</th>
</tr>
</thead>
</table>