

Installing, Configuring, and Upgrading vCloud Availability for Cloud-to- Cloud DR

April 2018

VMware vCloud Availability 1.0

VMware vCloud Availability for Cloud-to-Cloud DR



vmware®

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2018 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1 About Installing, Configuring, and Upgrading**
 - [vCloud Availability for Cloud-to-Cloud DR](#) 5
 - [Updated Information](#) 6
- 2 vCloud Availability for Cloud-to-Cloud DR Overview** 7
 - [vCloud Availability for Cloud-to-Cloud DR Services](#) 8
 - [vCloud Availability for Cloud-to-Cloud DR Services Requirements](#) 10
 - [vCloud Availability for Cloud-to-Cloud DR Network Port Configuration](#) 12
- 3 vCloud Availability for Cloud-to-Cloud DR Deployment Requirements** 17
- 4 Deploy vCloud Availability for Cloud-to-Cloud DR Services by Using the vSphere Web Client** 18
- 5 Deploy vCloud Availability for Cloud-to-Cloud DR Services by Using the OVF Tool** 21
- 6 Configuring vCloud Availability for Cloud-to-Cloud DR Services** 24
 - [Initial vCloud Availability for Cloud-to-Cloud DR Services Configuration](#) 24
 - [Configure a vCloud Availability Replicator](#) 24
 - [Configure a vCloud Availability Replication Manager](#) 25
 - [Configure a vCloud Availability vApp Replication Service/Manager](#) 26
 - [Configure a vCloud Availability Portal](#) 28
 - [Register a vCloud Availability Replicator with a vCloud Availability Replication Manager in the Same Site](#) 31
 - [Configure Cloud-to-Cloud Tunneling](#) 31
 - [Pair Cloud Sites](#) 34
- 7 Upgrading vCloud Availability for Cloud-to-Cloud DR** 36
 - [Order of Upgrading vCloud Availability for Cloud-to-Cloud DR Components](#) 36
 - [Upgrade vCloud Availability for Cloud-to-Cloud DR by Using the Downloadable ISO Image](#) 37
- 8 vCloud Availability for Cloud-to-Cloud DR Administration** 39
 - [Add a vCloud Availability Replicator](#) 39
 - [Replace the vCloud Availability vApp Replication Service/Manager Certificate with a CA-Signed Certificate](#) 40
 - [Replace the vCloud Availability Portal Certificate](#) 42

Configure vCloud Availability for Cloud-to-Cloud DR with a Renewed Lookup Service Certificate on a Platform Services Controller	43
Collect vCloud Availability for Cloud-to-Cloud DR Usage Information	45
Collecting Support Bundles for the vCloud Availability for Cloud-to-Cloud DR Components	46

About Installing, Configuring, and Upgrading vCloud Availability for Cloud-to- Cloud DR

1

The *Installing, Configuring, and Upgrading vCloud Availability for Cloud-to-Cloud DR* provides information on how to install, configure, and upgrade the VMware vCloud[®] Availability for Cloud-to-Cloud DR[™] solution.

Intended Audience

This information is intended for VMware Cloud Provider Program service providers and experienced system administrators who are familiar with virtual machine technology and data center operations including but not limited to the following areas:

- VMware vSphere[®]
- VMware vCloud Director[®]
- Secure Shell (SSH)
- Bash

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to <http://www.vmware.com/support/pubs>.

Updated Information

This *Installing, Configuring, and Upgrading vCloud Availability for Cloud-to-Cloud DR* document is updated with each release of the product or when necessary.

This table provides the update history of the *Installing, Configuring, and Upgrading vCloud Availability for Cloud-to-Cloud DR* document.

Revision	Description
9 OCT 2018	Updated the information in topic Configure Cloud-to-Cloud Tunneling .
2 AUG 2018	Added the following topics: <ul style="list-style-type: none">■ Chapter 7 Upgrading vCloud Availability for Cloud-to-Cloud DR■ Order of Upgrading vCloud Availability for Cloud-to-Cloud DR Components■ Upgrade vCloud Availability for Cloud-to-Cloud DR by Using the Downloadable ISO Image■ Collecting Support Bundles for the vCloud Availability for Cloud-to-Cloud DR Components
28 JUN 2018	Added the following topics: <ul style="list-style-type: none">■ vCloud Availability for Cloud-to-Cloud DR Network Port Configuration■ Add a vCloud Availability Replicator
8 JUN 2018	Initial release.

vCloud Availability for Cloud-to-Cloud DR Overview

2

The vCloud Availability for Cloud-to-Cloud DR solution provides replication and failover capabilities for vCloud Director workloads at both VM and vApp level.

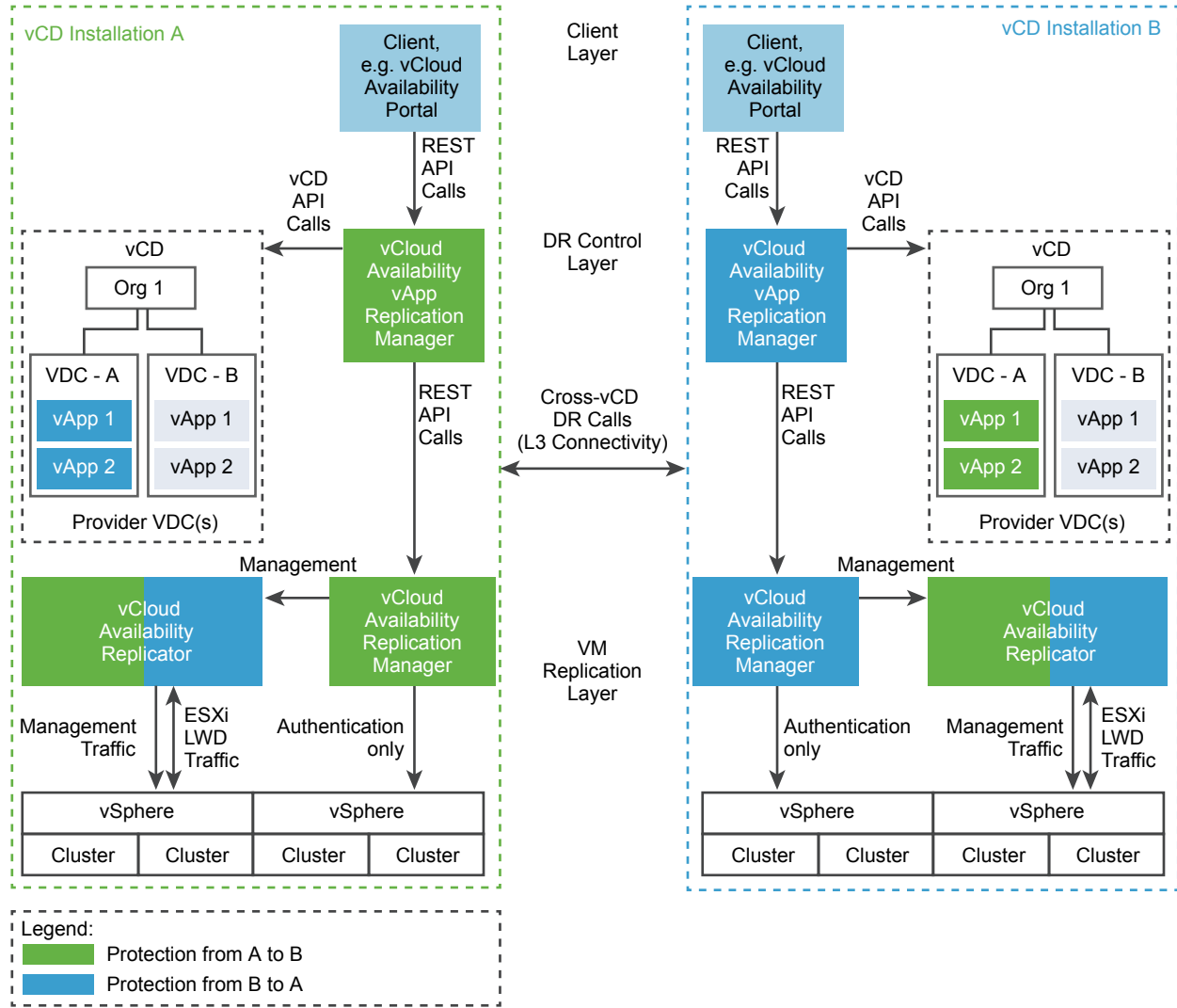
The service operates through a VMware Cloud Provider Program, and each installation provides recovery for multiple cloud environments. The vCloud Availability for Cloud-to-Cloud DR provides:

- Self-service protection and failover workflows per virtual machine (VM).
- Single installation package as a Photon-based virtual appliance.
- The capability of each deployment to serve as both source and recovery vCloud Director instance (site). There are no dedicated source and destination sites.
- Symmetrical replication flow that can be started from either the source or the recovery vCloud Director site.
- Replication and recovery of vApps and VMs between vCloud Director sites.
- Secure Tunneling through TCP proxy.
- Integration with existing vSphere environments.
- Multi-tenant support.
- Built-in encryption or encryption and compression of replication traffic.
- Support for multiple vCenter Server and ESXi versions.

The architecture of the solution relies on symmetrical replication operations between cloud environments. In a single cloud environment, the vCloud Availability Replicator, the vCloud Availability Replication Manager, and the vCloud Availability vApp Replication Service/Manager operate together to support replication, secure communication, and storage of the replicated data. Each service provider can support recovery for multiple customer environments that can scale to handle increasing loads for each tenant, and for multiple tenants.

For test and development purposes, you can employ the simplest architecture where all three vCloud Availability for Cloud-to-Cloud DR services are deployed and configured on a single appliance. For production deployments, you deploy and configure each service on a dedicated appliance.

The components without color in the following diagram represent existing components in the vCloud Director environments. The remaining colored cells represent vCloud Availability for Cloud-to-Cloud DR services that you deploy during vCloud Availability for Cloud-to-Cloud DR Installation and Configuration procedures.



This chapter includes the following topics:

- [vCloud Availability for Cloud-to-Cloud DR Services](#)
- [vCloud Availability for Cloud-to-Cloud DR Services Requirements](#)
- [vCloud Availability for Cloud-to-Cloud DR Network Port Configuration](#)

vCloud Availability for Cloud-to-Cloud DR Services

vCloud Availability for Cloud-to-Cloud DR is comprised of few services which are deployed and can coexist in the same virtual appliance.

Table 2-1. Services Definitions

Name	Description
vCloud Director	With the vCloud Director solution service providers can build secure, multi-tenant private clouds by pooling infrastructure resources into virtual data centers and exposing them to users through Web-based portals and programmatic interfaces as fully automated, catalog-based services.
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.
vCloud Availability Replicator	Exposes the low-level HBR primitives as REST APIs.
vCloud Availability Replication Manager	A management service operating on the vCenter Server level. It understands the vCenter Server level concepts for starting the replication workflow for the virtual machines.
vCloud Availability vApp Replication Service/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.
Light Weight Delta protocol (LWD Proxy)	The 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.
VMware Platform Services Controller [®]	The Platform Services Controller provides common infrastructure services to the vSphere environment. Services include licensing, certificate management, and authentication with VMware vCenter [®] Single Sign-On.
vCloud Availability Tunnel	Simplifies provider networking setup by channeling all incoming and outgoing traffic for a site through a single point - the vCloud Availability Tunnel appliance.
vCloud Availability Portal	The vCloud Availability 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 Portal also provides overall system and workload information.
vCloud Availability Portal Service	The vCloud Availability Portal Service provides authentication management, sessions management, disaster recovery workflow and state machine, and cache capabilities for the vCloud Availability Portal.
vCloud Configuration Portal	The vCloud Configuration Portal provides a graphic user interface to configure and manage the vCloud Availability Portal.

The vCloud Availability for Cloud-to-Cloud DR services provide a management interface for configuration and administration purposes. The following table can help you understand how to access the management interface of each service.

Table 2-2. Services Management Interface Addresses

Service	Management Interface Address and Port
vCloud Availability Replication Manager	https://Appliance-IP-Address:8044
vCloud Availability Replicator	https://Appliance-IP-Address:8043
vCloud Availability vApp Replication Service/Manager	https://Appliance-IP-Address:8046
vCloud Availability Portal	https://Appliance-IP-Address:8443

Table 2-2. Services Management Interface Addresses (Continued)

Service	Management Interface Address and Port
vCloud Configuration Portal	https://Appliance-IP-Address:5480
vCloud Availability Tunnel	https://Appliance-IP-Address:8047

You can find the configuration and log files for the vCloud Availability for Cloud-to-Cloud DR services at the following locations.

Table 2-3. Configuration Files Location

Service	Default Location
vCloud Availability Replication Manager	/opt/vmware/h4/manager/config/application.properties
vCloud Availability Replicator	/opt/vmware/h4/replicator/config/application.properties
vCloud Availability vApp Replication Service/Manager	/opt/vmware/h4/cloud/config/application.properties
vCloud Availability Portal	/opt/vmware/vcav-portal/conf/config.yml
vCloud Configuration Portal	/opt/vmware/vcav-portal-appliance/conf/serviceConfig.yml
vCloud Availability Tunnel	/opt/vmware/h4/tunnel/config/application.properties

Table 2-4. Log Files Location

Service	Default Location
vCloud Availability Replication Manager	/opt/vmware/h4/manager/log/manager.log
vCloud Availability Replicator	/opt/vmware/h4/replicator/log/replicator.log
vCloud Availability vApp Replication Service/Manager	/opt/vmware/h4/cloud/log/cloud.log
vCloud Availability Portal	/opt/vmware/vcav-portal/log/vcav-portal.log
vCloud Configuration Portal	/opt/vmware/vcav-portal-appliance/log/vcav-portal-appliance.log
vCloud Availability Tunnel	/opt/vmware/h4/tunnel/log/tunnel.log

vCloud Availability for Cloud-to-Cloud DR Services Requirements

Before you start deploying and configuring vCloud Availability for Cloud-to-Cloud DR services, verify that your environment meets the specific requirements.

vCloud Availability vApp Replication Service/Manager Users Requirements

The ESXi host port 902 must be open to proxy traffic to the consumer.

The vCloud Availability vApp Replication Service/Manager distinguishes between admin users and regular users. To start a session with administrator privileges, the credentials or SAML authenticator you enter for both of the vCloud Director sites must belong to the **ADMINISTRATORS** or **VRADMINISTRATORS** group. For example, the **Administrator@vsphere.local** SSO user you enter when logging into the management portal, is a member of the **ADMINISTRATORS** group.

You start an admin user session as a vCloud Director system user with the vCloud Director credentials or the SAML authenticator. Admin users can manage and monitor any vCloud Availability vApp Replication Service/Manager inventory object, and can manage the vCloud Availability vApp Replication Service/Manager appliance. As an admin user, you must extend your sessions. You get access to all vCloud Director sites when you authenticate successfully.

You start a regular user session as a vCloud Director user that is not a system user with vCloud Director credentials. Each regular user session is guaranteed to have a vCloud Director user and vCloud Director Org associated with the session. As a regular user, you can manage and monitor any vCloud Availability vApp Replication Service/Manager inventory object that belongs to the respective vCloud Director site. If you want to connect to multiple vCloud Director sites, you cannot manage the vCloud Availability vApp Replication Service/Manager appliance and you must explicitly extend your sessions.

You start a session on your local vCloud Director site, for example, *site1*. Disaster recovery operations require you to be logged into both sites, local and remote. To extend your current session, you log in to the remote vCloud Director site, for example, *site2*. Extending your current session allows the vCloud Availability vApp Replication Service/Manager client to communicate with the remote site and does not overwrite the session started on the local vCloud Director site. You extend your session within the vCloud Availability Portal interface by navigating to **Paired Clouds > Authentication Status**.

The following table lists vCloud Availability vApp Replication Service/Manager replication operations that require sessions on either of the sites or both.

Table 2-5. vCloud Availability vApp Replication Service/Manager Replication Operations with Required Sessions

Operation	Incoming Replication		Outgoing Replication	
	Required Session on Source Site	Required Session on Destination Site	Required Session on Source Site	Required Session on Destination Site
start	Yes	Yes	Yes	Yes
stop	No	Yes	Yes	Yes
reconfigure	No	Yes	Yes	Yes
failover	No	Yes	Yes	Yes
migrate	Yes	Yes	Yes	Yes
sync	No	Yes	Yes	Yes
pause	No	Yes	Yes	Yes
resume	No	Yes	Yes	Yes
reverse	Yes	Yes	Yes	Yes

Table 2-5. vCloud Availability vApp Replication Service/Manager Replication Operations with Required Sessions (Continued)

Operation	Incoming Replication		Outgoing Replication	
	Required Session on Source Site	Required Session on Destination Site	Required Session on Source Site	Required Session on Destination Site
failover test	No	Yes	Yes	Yes
failover test cleanup	No	Yes	Yes	Yes

Services Connectivity

- The vCloud Availability vApp Replication Service/Manager must have TCP access to vCloud Director, vCloud Availability Replication Manager, vCenter Server or PSC (depending on where the Lookup Service is hosted).
- 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.
- The vCloud Availability Replicator must have TCP access to the vCloud Availability Replication Manager, vCenter Server, and the Lookup Service.

Supported Topologies

The resource vCenter Server within a vCloud Director site must be within the same SSO domain. All vCloud Availability Replicator appliances within the respective site must be configured with that same SSO domain.

vCloud Availability for Cloud-to-Cloud DR Network Port Configuration

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

Network Port Configuration for Deployments Without Cloud-to-Cloud Tunneling

The following table shows the network ports required for a local site communication between vCloud Availability for Cloud-to-Cloud DR services.

Table 2-6. Network Ports for Local Site Connection Without Cloud-to-Cloud Tunneling

Source	Destination	Port Number	Protocol	Description
vCloud Availability Replicator service	Local ESXi hosts	80	HT TP S	Used to establish a connection between local vCloud Availability Replicator service and local ESXi hosts before initial replication starts.
vCloud Availability for Cloud-to-Cloud DR services that use single sign-on.	All Platform Services Controllers (PSC) in the same single sign-on domain. Used only if external PSC is used.	44 3	HT TP S	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.
vCloud Availability vApp Replication Service/Manager service or vCloud Availability Replicator service	All PSCs	74 44	TC P	Used for single sign-on and Lookup Service communication when vSphere 5.5 or later is used in the respective site.
vCloud Availability vApp Replication Service/Manager Service or vCloud Availability Replicator Service	Local vCenter Server	44 3	HT TP S	Used by the local vCloud Availability vApp Replication Service/Manager service or the vCloud Availability Replicator service for communication with the local vCenter Server.
vCloud Availability Replicator service	Local ESXi hosts	90 2	TC P and UD P	Used by the vCloud Availability Replicator service for replication traffic to the destination ESXi hosts.
Local ESXi hosts	Local LWD Proxy service	44 04 6	LW D	Used for replication data traffic from a protected ESXi host to the local LWD Proxy.

The following table shows the network ports required for external.

Table 2-7. Network Ports for External Communication Without Cloud-to-Cloud Tunneling

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

Network Port Configuration for Deployments with Cloud-to-Cloud Tunneling

The following table shows the network ports required for a local site communication between vCloud Availability for Cloud-to-Cloud DR services.

Table 2-8. Network Ports for Local Site Connection with Cloud-to-Cloud Tunneling

Source	Destination	Port Number	Protocol	Description
vCloud Availability Replicator service	Local ESXi hosts	80	HT TP S	Used to establish a connection between local vCloud Availability Replicator service and local ESXi hosts before initial replication starts.
vCloud Availability for Cloud-to-Cloud DR services that use single sign-on.	All Platform Services Controllers (PSC) in the same single sign-on domain. Used only if external PSC is used.	44 3	HT TP S	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.
vCloud Availability vApp Replication Service/Manager service or vCloud Availability Replicator service	All PSCs	74 44	TC P	Used for single sign-on and Lookup Service communication when vSphere 5.5 or later is used in the respective site.
vCloud Availability vApp Replication Service/Manager service or vCloud Availability Replicator service	Local vCenter Server	44 3	TC P	Used by the local vCloud Availability vApp Replication Service/Manager service or the vCloud Availability Replicator service for communication with the local vCenter Server.
vCloud Availability Replicator service	Local ESXi hosts	90 2	TC P and UD P	Used by the vCloud Availability Replicator service for replication traffic to the destination ESXi hosts.
Local ESXi hosts	Local LWD Proxy service	44 04 6	LW D	Used for replication data traffic from a protected ESXi host to the local LWD Proxy.
vCloud Availability Tunnel appliance	Local LWD Proxy service	44 04 5	LW DS	Used for replication data traffic from the vCloud Availability Tunnel to all local vCloud Availability Replicator instances.
vCloud Availability Tunnel appliance	vCloud Availability vApp Replication Service/Manager service	80 46	HT TP S	vCloud Availability vApp Replication Service/Manager service management from the vCloud Availability Tunnel appliance.
vCloud Availability Tunnel appliance	vCloud Availability Replicator service	80 43	HT TP S	vCloud Availability Replicator management from the vCloud Availability Tunnel.
vCloud Availability Tunnel	vCloud Availability Replication Manager	80 44	HT TP S	Used for management traffic from the vCloud Availability Tunnel to the vCloud Availability Replication Manager within a site.

The following table shows the network ports required for an external communication.

Table 2-9. Network Ports for External Communication with Cloud-to-Cloud Tunneling

Source	Destination	Port Number	Protocol	Description
Public Network	vCloud Availability Tunnel appliance	8048	Any	Replication management and data traffic from a source site to the local vCloud Availability Tunnel appliance.

vCloud Availability for Cloud-to-Cloud DR Deployment Requirements

3

Before you start deploying and configuring vCloud Availability for Cloud-to-Cloud DR services, verify that your environment complies with the following requirements.

Requirements

- If your ESXi hosts have more than one NIC, make sure that *vSphere Replication NFC Traffic* is enabled. This setting is required for routing the replication traffic. If *vSphere Replication NFC Traffic* is not enabled, you might get timeout errors during replication setup or reconfiguration. For more information about enabling *vSphere Replication NFC Traffic*, see [Set Up a VMkernel Adapter for vSphere Replication Traffic on a Target Host](#) in the *VMware vSphere Replication Administration Guide*.
- The vCloud Availability vApp Replication Service/Manager deployment requires two sites, for example *site1* and *site2*.
- Each of the sites consists of a vCloud Director installation and a resource vCenter Server with at least one ESXi host.

In the current example, during the deployment and configuration, *site1* is considered as source and consists of *vCD1*, *VC1*, and *Org1*. *Site2* is considered as destination and consists of *vCD2*, *VC2*, and *Org2*. After you deploy and configure all vCloud Availability for Cloud-to-Cloud DR services, you can replicate VMs and vApps from **site1** to **site2**, and from **site2** to **site1**.

Note The vCloud Availability for Cloud-to-Cloud DR services perform a host name certificate verification. Therefore, it is expected that the `CommonName` 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.

Deploy vCloud Availability for Cloud-to-Cloud DR Services by Using the vSphere Web Client

4

This procedure demonstrates how to deploy all cloud services providing disaster recovery with a single installer appliance by using the vSphere Web Client.

You install all vCloud Availability for Cloud-to-Cloud DR services by using a single installation OVA package. Depending on your deployment requirements, you can select various deployment types. The following table can help you understand what the different deployment types include.

Table 4-1. vCloud Availability for Cloud-to-Cloud DR Deployment Types

Deployment Type	Description
Combined	All-in-one deployment type that is suitable for testing, evaluation, and small deployments. You deploy a single appliance in an environment configuration of 4 vCPUs, 6 GB RAM, and 10 GB storage, with all vCloud Availability for Cloud-to-Cloud DR services ready for configuration.
Manager node with vCloud Director support	Used for a deployment of a vCloud Availability Replication Manager service and a vCloud Availability vApp Replication Service/Manager service in a single appliance in an environment configuration of 4 vCPUs, 6 GB RAM, and 10 GB storage. The vCloud Availability Portal and the vCloud Configuration Portal are running on this node.
Replicator node	Used for a deployment of a dedicated vCloud Availability Replicator appliance in an environment configuration of 2 vCPUs, 4 GB RAM, and 10 GB storage.
Large Replicator node	Used for a deployment of a dedicated vCloud Availability Replicator appliance in an environment configuration of 4 vCPUs, 6 GB RAM, and 10 GB storage.
Tunnel node	Used for a deployment of a vCloud Availability Tunnel appliance in an environment configuration of 2 vCPUs, 4 GB RAM, and 10 GB storage.

Prerequisites

- Obtain the installation OVA package that contains all the vCloud Availability for Cloud-to-Cloud DR appliances binaries.
- If you deploy an OVF template for the first time, download and install the Client Integration Plug-in through the `Deploy OVF Template` in the vSphere Web Client.

Procedure

- 1 Log in to the vSphere Web Client.

- 2 Right-click the target location (data center, folder, cluster, resource pool, or host) where you want to deploy the vCloud Availability for Cloud-to-Cloud DR services and select **Deploy OVF Template** from the drop-down menu.

The **Deploy OVF Template** wizard opens.

- 3 In the **Select source** page, browse to the installation package location.

The syntax of the OVA filename is `vCloud-Availability-C2C-release_number-xxx-build_number_OVF10.ova`.

- 4 Click **Next** and review the details.
- 5 Read and accept the license agreement, and click **Next**.
- 6 In the **Select name and folder** page, enter a name for the appliance, the data center, or data center folder that contains the host or cluster on which you want to deploy the appliance.
- 7 Click **Next**.
- 8 In the **Select configuration** page, leave the default **Combined** deployment configuration and click **Next**.

The **Combined** deployment creates a single virtual appliance that hosts all vCloud Availability for Cloud-to-Cloud DR services.

Note Use this option for test and development deployments. For production environments, deploy and configure a dedicated appliance for each vCloud Availability for Cloud-to-Cloud DR service.

- 9 In the **Select a resource** page, select the target host, or cluster where the vCloud Availability for Cloud-to-Cloud DR services are about to run and click **Next**.
- 10 Select the virtual disk format and the storage policy for the appliance from the drop-down menu.
Thick Provision Lazy Zeroed and Datastore Default are selected by default.
- 11 In the **Setup network** page, enter the settings for connecting the vCloud Availability for Cloud-to-Cloud DR appliance to the network.
 - a Select the source network that the vCloud Availability for Cloud-to-Cloud DR appliance uses.
VM Network is used by default.
 - b Select the protocol version for the appliance IP address.
IPv4 is selected by default.
 - c Select how to allocate the IP address of the appliance
Static – Manual is used by default.

12 Customize the deployment properties of the vCloud Availability for Cloud-to-Cloud DR appliance in the **Customize template** page and click **Next**.

- a (Optional) Select the `Enable SSH` check box.
- b In the `NTP Server` section, enter the NTP server address that the appliance uses.

Important Make sure that vCenter Server, ESXi, vCloud Director, the Platform Services Controller, and all vCloud Availability for Cloud-to-Cloud DR appliances use the same NTP server.

- c In the `root password` section, enter and confirm the password of the `root` user for the appliance. `vmware` is used by default. If you leave the `root password` section empty, the default password is set for the `root` user.

Note After you install the combined appliance and you log in for the first time, you are prompted to change the `root` password. You must create a secured password with a minimum of eight characters and containing at least one of the following:

- Lowercase: a b c
 - Uppercase: A B C
 - Numeric: 1 2 3
 - Special: & # %
-

13 Review all the settings configured for the installer appliance, select **Power on after deployment**, and click **Finish** to begin the OVA installation process.

The wizard closes.

The **Recent Tasks** page shows the status for initializing the OVF deployment on the target host.

Deploy vCloud Availability for Cloud-to-Cloud DR Services by Using the OVF Tool

5

This procedure demonstrates how to deploy vCloud Availability for Cloud-to-Cloud DR services by using the VMware OVF Tool. Alternatively, you can use the vSphere Web Client to install the vCloud Availability for Cloud-to-Cloud DR services.

You install all vCloud Availability for Cloud-to-Cloud DR services by using a single installation OVA package. Depending on your deployment requirements, you can select various deployment types. The following table can help you understand what the different deployment types include.

Table 5-1. vCloud Availability for Cloud-to-Cloud DR Deployment Types

Deployment Type	Description
Combined	All-in-one deployment type that is suitable for testing, evaluation, and small deployments. You deploy a single appliance in an environment configuration of 4 vCPUs, 6 GB RAM, and 10 GB storage, with all vCloud Availability for Cloud-to-Cloud DR services ready for configuration.
Manager node with vCloud Director support	Used for a deployment of a vCloud Availability Replication Manager service and a vCloud Availability vApp Replication Service/Manager service in a single appliance in an environment configuration of 4 vCPUs, 6 GB RAM, and 10 GB storage. The vCloud Availability Portal and the vCloud Configuration Portal are running on this node.
Replicator node	Used for a deployment of a dedicated vCloud Availability Replicator appliance in an environment configuration of 2 vCPUs, 4 GB RAM, and 10 GB storage.
Large Replicator node	Used for a deployment of a dedicated vCloud Availability Replicator appliance in an environment configuration of 4 vCPUs, 6 GB RAM, and 10 GB storage.
Tunnel node	Used for a deployment of a vCloud Availability Tunnel appliance in an environment configuration of 2 vCPUs, 4 GB RAM, and 10 GB storage.

For more information about working with the OVF Tool, see the [OVF Tool User's Guide](#).

Prerequisites

Obtain the installation OVA package that contains all the vCloud Availability for Cloud-to-Cloud DR appliances binaries.

Procedure

1 Define deployment variables.

```
# OVA="local_client_path/vCloud-Availability-C2C-release_number-xxx-build_number_OVF10.ova"

# VMNAME='Name-to-be-Assigned-to-the-VM'

# DATASTORE="vsphere-datastore"

# VSPHERE_NETWORK="VM-Network"

# VSPHERE_ADDRESS=vsphere-ip-address

# VSPHERE_USER=vsphere-admin-user

# VSPHERE_LOCATOR="vsphere-locator"
```

The `VSPHERE_LOCATOR` value contains the target data center name, the tag `host`, the name of the target cluster, and the IP address or the fully qualified domain name (FQDN) of the target ESXi host. The `VSPHERE_LOCATOR` value depends on the topology of your vSphere environment. Following are examples for valid `VSPHERE_LOCATOR` values.

- `/data-center-name/host/cluster-1-name/fully-qualified-domain-name`
- `/data-center-name/host/cluster-2-name/host-IP-address`

If the target ESXi host is not part of a cluster, skip the `cluster-name` element, as shown in the following examples.

- `/data-center-name/host/fully-qualified-domain-name`
- `/data-center-name/host/host-IP-address`

The `VSPHERE_DATASTORE` value is the datastore name as it is displayed in the vSphere Web Client.

For more information about the `VSPHERE_LOCATOR` value, run the `./ovftool --help locators` command.

For more information about working with the OVF Tool, see the [OVF Tool User's Guide](#).

2 Deploy a vCloud Availability for Cloud-to-Cloud DR appliance.

The following example command deploys a Combined vCloud Availability for Cloud-to-Cloud DR appliance and sets static IP addresses.

```
# echo $VMNAME

# ./ovftool/ovftool --name="{VMNAME}" --datastore="{DATASTORE}" --acceptAllEulas --powerOn --
X:enableHiddenProperties --X:injectOvfEnv --X:waitForIp --ipAllocationPolicy=fixedPolicy --
deploymentOption=combined --machineOutput --noSSLVerify --overwrite --powerOffTarget --
prop:guestinfo.cis.appliance.root.password='Your-Root-Password' --
prop:guestinfo.cis.appliance.ssh.enabled=True --prop:guestinfo.cis.appliance.net.ntp=your-ntp-
server --prop:vami.DNS.VMware_vCloud_Availability_for_Cloud-to-Cloud_DR=Your-DNS-Server-Address --
```

```
prop:vami.domain.VMware_vCloud_Availability_for_Cloud-to-Cloud_DR=Your-Domain-Name --  
prop:vami.gateway.VMware_vCloud_Availability_for_Cloud-to-Cloud_DR=Your-Gateway-IP-Address --  
prop:vami.ip0.VMware_vCloud_Availability_for_Cloud-to-Cloud_DR=IP-to-be-Assigned-to-the-Appliance  
--prop:vami.netmask0.VMware_vCloud_Availability_for_Cloud-to-Cloud_DR=Your-Netmask-Address  
--prop:vami.searchpath.VMware_vCloud_Availability_for_Cloud-to-Cloud_DR=Your-Search-Path-Address  
"--net:VM Network=${VSPHERE_NETWORK}" --diskMode=thin "${OVA}" "vi://${  
{VSPHERE_USER}:VSPHERE_USER_PASSWORD@${VSPHERE_ADDRESS}${VSPHERE_LOCATOR}"
```

The **Recent Tasks** page shows the status for initializing the OVF deployment on the target host.

Configuring vCloud Availability for Cloud-to- Cloud DR Services

6

To configure the vCloud Availability for Cloud-to-Cloud DR solution, you perform an initial configuration of the vCloud Availability Replicator, vCloud Availability Replication Manager, and vCloud Availability vApp Replication Service/Manager, register the services within a single site, then pair two cloud sites.

The vCloud Availability Portal is configured automatically during deployment and configuration of the remaining vCloud Availability for Cloud-to-Cloud DR components. After you configure all vCloud Availability for Cloud-to-Cloud DR services in both cloud sites, you can log in to the vCloud Availability Portal at `https://Appliance-IP-address:8443`. Tenant user names use the `user@org` format.

A best practice is to configure all services in one site, then register the vCloud Availability Replicator with the vCloud Availability Replication Manager in the same site. Then perform the initial configuration and registration on the second site.

This chapter includes the following topics:

- [Initial vCloud Availability for Cloud-to-Cloud DR Services Configuration](#)
- [Register a vCloud Availability Replicator with a vCloud Availability Replication Manager in the Same Site](#)
- [Configure Cloud-to-Cloud Tunneling](#)
- [Pair Cloud Sites](#)

Initial vCloud Availability for Cloud-to-Cloud DR Services Configuration

Every vCloud Availability for Cloud-to-Cloud DR service has a dedicated service management UI. When you log in to a vCloud Availability for Cloud-to-Cloud DR service management UI for the first time after deployment, the initial configuration wizard starts.

Configure a vCloud Availability Replicator

To configure a vCloud Availability Replicator, you change the initial password that you set during the OVA deployment, and register the vCloud Availability Replicator appliance to a Lookup service.

Procedure

- 1 In a Web browser, go to `https://Appliance-IP-address:8043`.
The *VMware vCloud[®] Availability Replicator Server Getting Started* page opens.
- 2 If you are prompted for Client Certificate, click **Cancel**.
- 3 Click **VMware vCloud[®] Availability Replicator Configuration Portal**.
You are redirected to the Replicator Configuration Portal page.
- 4 Log in using the *root* password that you set during the OVA deployment.
The **Change Appliance Root Password** pane opens.
- 5 Change the initial appliance password and click **Next**.
Note the new password, as you need it to configure the other vCloud Availability for Cloud-to-Cloud DR services.
The **Setup Lookup service** pane opens.
- 6 Enter a valid lookup service address and click **Next**.
Enter the lookup service address in the following format `https://Appliance-IP-address:port-number/lookupservice/sdk`.
- 7 Review the lookup service certificate details and click **Accept**.
- 8 To complete the initial vCloud Availability Replicator configuration, click **Finish**.
You are redirected to the vCloud Availability Replicator health status page.

What to do next

You can now perform an initial configuration of the vCloud Availability Replication Manager. For more information, see [Configure a vCloud Availability Replication Manager](#).

Configure a vCloud Availability Replication Manager

To configure a vCloud Availability Replication Manager, register the vCloud Availability Replication Manager appliance to a Lookup service.

Procedure

- 1 In a Web browser, go to `https://Appliance-IP-address:8044`.
The *VMware vCloud[®] Replication Manager Getting Started* page opens.
- 2 If you are prompted for Client Certificate, click **Cancel**.
- 3 Click **VMware vCloud[®] Availability Replication Manager Configuration Portal**.
You are redirected to the Replication Manager Configuration Portal login page.

- 4 Log in with the appliance *root* password that you set during the initial vCloud Availability Replicator configuration.

You are redirected to the vCloud Availability Replication Manager health status page with an indication that Lookup service settings are missing.

- 5 Navigate to **Configuration > Set lookup service**.
- 6 Enter a valid Lookup service address and click **OK**.

Enter the Lookup service address in the following format `https://Appliance-IP-address:port-number/lookupservice/sdk`.

- 7 Review the Lookup service certificate details and click **Accept**.

What to do next

You can now perform an initial configuration of the vCloud Availability vApp Replication Service/Manager. For more information, see [Configure a vCloud Availability vApp Replication Service/Manager](#).

Configure a vCloud Availability vApp Replication Service/Manager

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

Procedure

- 1 In a Web browser, go to `https://Appliance-IP-address:8046`.

The *VMware vCloud[®] Availability vApp Replication Manager Server Getting Started* page opens.

- 2 If you are prompted for Client Certificate, click **Cancel**.
- 3 Log in with the appliance *root* password that you set during the initial vCloud Availability vApp Replication Service/Manager configuration.

You are redirected to the vCloud Availability vApp Replication Service/Manager initial configuration wizard.

- 4 Enter a Site Name and Site Description, and click **Next**.

Note the Site Name, as the name you enter here is used as an identifier later and cannot be changed.

- 5 Enter a valid Lookup service address and click **Next**.

Enter the Lookup service address in the following format `https://PSC-IP-address:port-number/lookupservice/sdk`.

- 6 Review the lookup service certificate details and click **Accept**.

7 Set up the vCloud Availability Replication Manager.

- a Enter a Manager URL in the following format: `https://Manager-IP-Address:8044`

Note The Manager URL is not mandatory when you performed the combined appliance deployment type. The combined appliance contains the vCloud Availability Replication Manager used for the vCloud Availability vApp Replication Service/Manager initial configuration. If you omit the vCloud Availability Replication Manager endpoint, configuration operations assume that the vCloud Availability Replication Manager services are running on the same appliance, listening on the same port - 8044.

- b Enter SSO user name and SSO password and click **Next**.

These credentials are used to connect to and exchange information with vCenter Server. This account is also used as an administrative vCloud Availability vApp Replication Service/Manager account.

Important The SSO user you enter must belong to the vCenter Server **ADMINISTRATORS** or the **VRADMINISTRATORS** group.

8 Review the vCloud Availability Replication Manager certificate details and click **Accept**.

9 Set up vCloud Director.

- a Select the Configuration Type and click **Next**.

Note

- Leave the default **Automatic** configuration type if vCloud Director is federated with a previously specified Lookup Service, there is only one registered vCloud Director in the Lookup service and the SSO user belongs to the System Administrator group in vCloud Director.
 - If vCloud Director is not federated with a previously specified Lookup Service, select to manually configure the vCloud Availability vApp Replication Service/Manager.
-

- b Enter vCloud Director URL in the following format: `https://vCloud Director-IP-Address:443/api`.

- c Enter vCloud Director system administrator user name and password to perform all management operations, and click **Next**.

The expected format for the user name is `user@system`.

10 Review the vCloud Director certificate details and click **Accept**.

Note This step is not present for the **Automatic** configuration type.

The initial configuration of all disaster recovery services is complete.

11 Review the vCloud Availability vApp Replication Service/Manager configuration summary and click **Finish**.

- 12 (Optional) Verify that the vCloud Availability vApp Replication Service/Manager service is successfully configured.
 - a Go to the **Diagnostics** tab and verify that there are no errors or alerts.
 - b Click **Details** next to Manager.
 - c Verify that at least one vCloud Availability Replicator is listed per site.

What to do next

If your deployment requires more than one vCloud Availability Replicator, you can [Add a vCloud Availability Replicator](#).

You can also proceed with [Register a vCloud Availability Replicator with a vCloud Availability Replication Manager in the Same Site](#).

Configure a vCloud Availability Portal

You use the vCloud Configuration Portal to configure the vCloud Availability Portal Service.

Prerequisites

Verify that the following vCloud Availability for Cloud-to-Cloud DR services are deployed:

- vCloud Availability vApp Replication Service/Manager
- vCloud Availability Portal
- vCloud Configuration Portal

For more information about deploying vCloud Availability for Cloud-to-Cloud DR services, see [Chapter 4 Deploy vCloud Availability for Cloud-to-Cloud DR Services by Using the vSphere Web Client](#) and [Chapter 5 Deploy vCloud Availability for Cloud-to-Cloud DR Services by Using the OVF Tool](#).

Procedure

- 1 In a Web browser, go to the vCloud Configuration Portal at `https://Appliance-IP-Address:5480`.
- 2 Log in using the *root* password that you set during the OVA deployment.

The *vCloud Configuration Portal Initial Setup* page opens.
- 3 In the *vApp RM/vCD Connection* tab, enter the vCloud Availability vApp Replication Service/Manager and vCloud Director details.
 - a Enter the vCloud Availability vApp Replication Service/Manager endpoint address in the `https://hostname:port` format.
 - b Enter a vCloud Director **system administrator** user name and password.

You can enter the details of a local or SSO user.
 - c If you are using an SSO user, select the **SSO User** check box.
 - d Click **Connect**.

- e Review the vCloud Availability vApp Replication Service/Manager certificate details and click **Accept**.

A *Connection succeeded* message appears.

vCloud Director Base URL and Web Console addresses appear. If you use an SSO account, the Lookup Service endpoint address also appears.

- f To verify that vCloud Availability vApp Replication Service/Manager and vCloud Director connection is successfully established, click **Test**.

A *Test Result* pop-up window opens.

Verify that *Fetch vCD Token* and *Connect to vApp RM* tests complete successfully. If you use an SSO account, verify that the *Fetch HoK Token* test also completes successfully.

- g After the connection test completes, click **Done**.

A *Test succeeded* message appears.

- h Click **Next**.

4 In the *Database Connection* tab, set up a database.

- a Enter the details for your database.

You can use an embedded database that is hosted in the vCloud Availability Portal VM or a custom database.

Option	Description
(Optional) Embedded	If you use the database that is embedded in the vCloud Availability Portal, select the Enable Reconfiguration check box.
Custom	If you use a custom database, enter the following details: <ul style="list-style-type: none"> ■ Host address ■ Port number ■ Database Name ■ User Name ■ Password

- b To verify that the database is properly configured, click **Test**.

After a successful verification, a *Test succeeded* message appears.

- c Click **Next**.

- 5 In the *Portal Service Configuration* tab, configure the vCloud Availability Portal Service.
 - a (Optional) You can change the default 8443 port.

Important If you change the default vCloud Availability Portal port, you must manually modify the firewall rules for the VM that hosts the vCloud Availability Portal Service.

- b (Optional) To replace the vCloud Availability Portal certificate by clicking **Replace**.
A *Replace Certificate* pop-up window opens.
 - c Replace the vCloud Availability Portal certificate.

Note If you are using a custom certificate, make sure that the certificate .pem file contains both a private key and certificate.

Option	Description
Auto Generate	To generate a new SSL certificate for vCloud Availability Portal, click Auto Generate .
Upload	To upload a third-party certificate, click Upload and select the certificate .pem file.
Certificate Panel	You can also copy the content of the certificate .pem file and paste it in the <i>Certificate Panel</i> .

- d (Optional) If you generated a new or uploaded a third-party certificate, click **OK**.
- 6 In the *Portal Service Configuration* tab, click **Start Service**.

A *Running Progress* pop-up window appears.

- 7 Verify that the initial vCloud Availability Portal configuration is successful.

The *Running Progress* pop-up window should display green ticks for the following configuration areas:

- a Setup Database
- b Update vApp RM Configuration
- c Update Portal Service Configuration
- d Update Portal Service Certificate
- e Test Portal Service Connection

If the verification fails before *Test Portal Service Connection* is verified, click **Cancel** to close the *Running Progress* window, and reconfigure the vCloud Availability Portal from the beginning.

If the verification fails at *Test Portal Service Connection*, click **Go to Support Bundle** and generate a support bundle, to troubleshoot any issues.

- 8 If checkmarks are green, click **Done**.
You are redirected to the vCloud Configuration Portal Home page.

After the initial vCloud Availability Portal configuration completes successfully, you are redirected to the vCloud Configuration Portal Home page where you can monitor the vCloud Availability Portal system health. You can also modify the existing vCloud Availability Portal configuration.

Note If you update the vCloud Availability Portal database configuration, you must also reconfigure the vCloud Availability vApp Replication Service/Manager settings. In the vCloud Configuration Portal, go to the **vApp RM** tab, click **Edit**, and enter the vCloud Availability vApp Replication Service/Manager details.

Register a vCloud Availability Replicator with a vCloud Availability Replication Manager in the Same Site

You register a vCloud Availability Replicator to a vCloud Availability Replication Manager in the same site, so that the two services can work together.

Prerequisites

Verify that you have configured a vCloud Availability Replicator appliance and a vCloud Availability Replication Manager appliance in the same site.

Procedure

- 1 In a Web browser, go to `https://Appliance-IP-address:8044`.
The *VMware vCloud[®] Replication Manager Getting Started* page opens.
- 2 Click **VMware vCloud[®] Availability Replication Manager Configuration Portal**.
You are redirected to the VMware vCloud[®] Availability Replication Manager Configuration Portal login page.
- 3 Log in with the appliance password that you set during the initial vCloud Availability Replicator configuration.
- 4 Navigate to **Replicators > New replicator**.
- 5 In the **Replicators administration** pane, provide the vCloud Availability Replicator details and click **OK**.
If you enter the vCloud Availability Replicator FQDN, for example `eu-2.replicator.com`, the VMware vCloud[®] Availability Replication Manager Configuration Portal displays the vCloud Availability Replicator appliance IP address instead of the FQDN.

Configure Cloud-to-Cloud Tunneling

To establish a secure connection between two data centers, you can optionally configure Cloud-to-Cloud Tunneling.

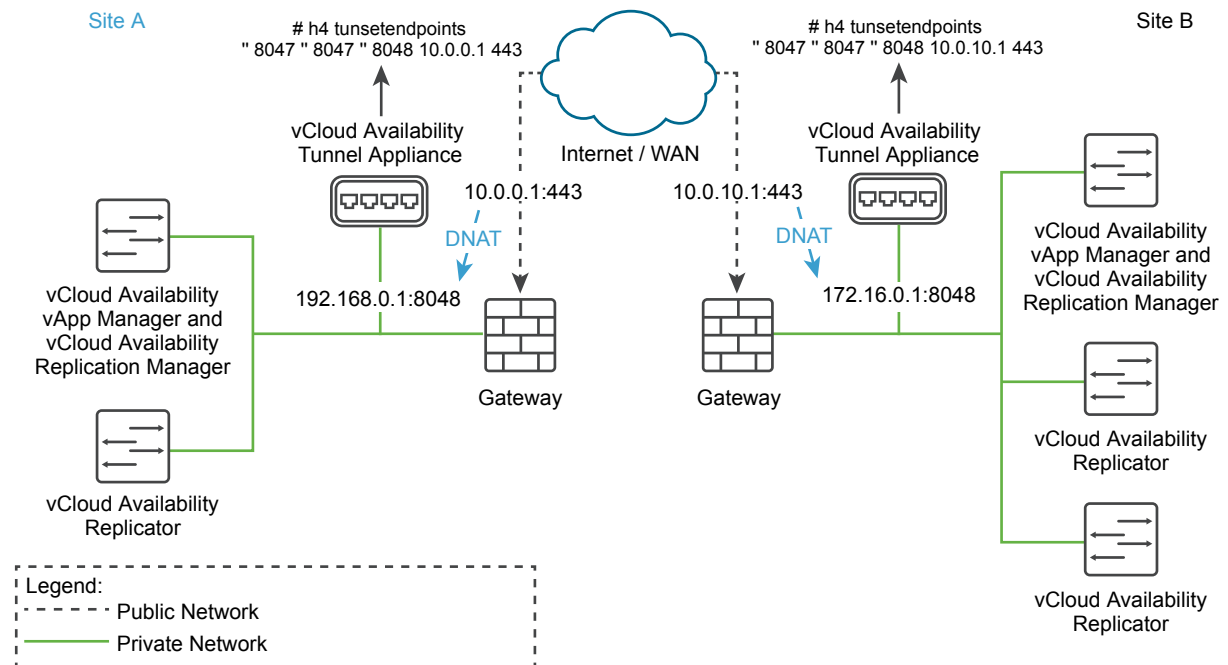
vCloud Availability for Cloud-to-Cloud DR requires that each component on a local site has bidirectional TCP connectivity to each component on the remote site. For example, each vCloud Availability Replicator in the local site communicates with the vCloud Availability Replication Manager in the remote 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 a problem, 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 cross-site traffic goes through the vCloud Availability Tunnel appliances.

Network Requirements

Expose a public endpoint for every vCloud Availability Tunnel. Every local vCloud Availability Tunnel appliance must be reachable for remote TCP clients. By default, the public endpoint of the vCloud Availability Tunnel appliance is 8048. You must set an IP and port in the local site that is reachable for remote sites and forward it to the private address of the vCloud Availability Tunnel appliance, port 8048, for example, by using destination network address translation(DNAT).

The following demonstrates a deployment where a Cloud-to-Cloud Tunneling is configured.



Prerequisites

- Verify that you have deployed the following appliances:
 - vCloud Availability Replication Manager
 - vCloud Availability Replicator
 - vCloud Availability vApp Replication Service/Manager
 - vCloud Availability Tunnel

For more information, see [Chapter 4 Deploy vCloud Availability for Cloud-to-Cloud DR Services by Using the vSphere Web Client](#).

- For both sites, verify that you have locally registered the vCloud Availability Replicator to a vCloud Availability Replication Manager. For more information, see [Register a vCloud Availability Replicator with a vCloud Availability Replication Manager in the Same Site](#).

Procedure

- 1 Log in to the vCloud Availability Tunnel appliance.
 - a Open an SSH connection to the vCloud Availability Tunnel appliance.
 - b Log in as **root**.
- 2 Configure vCloud Availability Tunnel public endpoints.

```
$ h4 tunloginroot 'Tunnel-Appliance-Root-Password'

$ h4 tunsetendpoints private-mgmt-address private-mgmt-port public-mgmt-address public-mgmt-port
private-tunnel-address private-tunnel-port public-tunnel-address public-tunnel-port
```

The following table describes the `tunsetendpoints` command arguments:

Option	Description
<code>private-mgmt-address</code>	The address of the tunneling service management endpoint that is used by components on the local site. It is a best practice to leave this blank.
<code>private-mgmt-port</code>	The port of the tunneling service management endpoint that is used by components on the local site. The default configuration uses port 8047.
<code>public-mgmt-address</code>	The address of the tunneling service management endpoint that is used by components on the remote site. It is a best practice to leave this blank.
<code>public-mgmt-port</code>	The port of the tunneling service management endpoint that is used by components on the remote site. The default configuration uses port 8047.
<code>private-tunnel-address</code>	The address of the tunnel endpoint that is used by components on the local site. It is a best practice to leave this blank.
<code>private-tunnel-port</code>	The port of the tunnel endpoint that is used by components on the local site. The default configuration uses port 8048.
<code>public-tunnel-address</code>	If you have configured port forwarding, for example DNAT, for this site, enter the public address. If you have not configured port forwarding, leave this blank.
<code>public-tunnel-port</code>	If you have configured port forwarding, for example DNAT, for this site, enter the public port. If you have not configured port forwarding, enter 8048.

The following example demonstrates the `h4 tunsetendpoints` command where port 443 is the destination network address translation (DNAT) port of the vCloud Availability Tunnel public endpoint:

```
$ h4 tunsetendpoints '' 8047 '' 8047 '' 8048 Public-Endpoint-Address 443
```

- 3 Export the vCloud Availability Tunnel certificate from the certificate store.

```
$ keytool -importkeystore -srckeystore /opt/vmware/h4/tunnel/config/keystore.jks -srcstorepass "$
(grep keystore.password /opt/vmware/h4/cloud/config/application.properties | awk -F = '{print
$2}')" -destkeystore /tmp/tunnel.p12 -deststoretype PKCS12 -deststorepass temporarySecret -
destkeypass temporarySecret; openssl pkcs12 -in /tmp/tunnel.p12 -nokeys -out /tmp/tunnel.pem
```

- 4 Save the `/tmp/tunnel.pem` file locally to your work station.
- 5 Log in to the vCloud Availability vApp Replication Service/Manager appliance console.
 - a Open an SSH connection to the vCloud Availability vApp Replication Service/Manager appliance.
 - b Log in as **root**.
- 6 Upload the `tunnel.pem` file to the `/tmp` folder of the vCloud Availability vApp Replication Service/Manager appliance.
- 7 Register the vCloud Availability Tunnel appliance to the vCloud Availability vApp Replication Service/Manager appliance.

```
$ c4 loginroot 'Tunnel-Appliance-Root-Password'

$ c4 regtunnel https://Tunnel-IP-Address:8047 "$(cat /tmp/tunnel.pem)" 'Tunnel-Appliance-Root-Password'
```

- 8 Reboot the vCloud Availability vApp Replication Service/Manager service.
 - a In a Web browser, go to `https://Appliance-IP-address/ui/admin`.
 - b Log in as **root**.
 - c In the **System Monitoring** tab, click **Restart Service**.

If you deployed a Combined appliance, you can skip the next step. If you have dedicated vCloud Availability Replicator appliances, you must reboot the vCloud Availability Replicator service on every vCloud Availability Replicator appliance in the site.

- 9 Reboot the vCloud Availability Replicator service.
 - a In a Web browser, go to `https://Appliance-IP-address:8043`.
 - b Enter the appliance *root* password.
 - c In the **System Monitoring** tab, click **Restart Service**.

What to do next

After you configure Cloud-to-Cloud Tunneling in both vCloud Availability for Cloud-to-Cloud DR sites, you can pair your cloud sites. For more information, see [Pair Cloud Sites](#).

Pair Cloud Sites

You establish a trust between vCloud Availability vApp Replication Service/Manager instances in two different sites.

You can initiate a cloud sites pairing from either one of the sites that you want to establish a trust between.

Prerequisites

Verify that you have deployed and configured a vCloud Availability Replicator and a vCloud Availability Replication Manager in both sites you are establishing a trust between.

Procedure

- 1 In a Web Browser, go to the vCloud Availability vApp Replication Service/Manager Configuration Portal at `https://Appliance-IP-Address:8046`.
- 2 Navigate to **Sites > New site**.
- 3 In the Sites administration pane, enter the site vCloud Availability vApp Replication Service/Manager details and click **OK**.

Note If you are using Cloud-to-Cloud Tunneling, you must enter the API URL with port 8048, for example `https://tunneling-appliance-IP-address:8048`.

- 4 To verify that the trust between the two sites is successfully established, navigate to **Sites > Show all sites**.

The new site appears in the **Sites administration** pane.

- 5 To verify the vCloud Availability vApp Replication Service/Manager status, navigate to **Diagnostics > Health > Site Statuses**.

Upgrading vCloud Availability for Cloud-to- Cloud DR



You upgrade all vCloud Availability for Cloud-to-Cloud DR components by using a downloadable ISO image.

The downloadable ISO image is the only means of upgrading from vCloud Availability for Cloud-to-Cloud DR 1.0 to vCloud Availability for Cloud-to-Cloud DR 1.0.1.

This chapter includes the following topics:

- [Order of Upgrading vCloud Availability for Cloud-to-Cloud DR Components](#)
- [Upgrade vCloud Availability for Cloud-to-Cloud DR by Using the Downloadable ISO Image](#)

Order of Upgrading vCloud Availability for Cloud-to-Cloud DR Components

To upgrade vCloud Availability for Cloud-to-Cloud DR, you must upgrade vCloud Availability for Cloud-to-Cloud DR components in a specific order.

You can upgrade vCloud Availability for Cloud-to-Cloud DR components in one site and then upgrade all components in the peer site. vCloud Availability for Cloud-to-Cloud DR 1.0 components can work with vCloud Availability for Cloud-to-Cloud DR 1.0.1 components and your replications remain functional and manageable. During the upgrade of one of the peer sites, you might observe replication interruptions and Recovery Point Objective (RPO) violations.

You can also upgrade vCloud Availability for Cloud-to-Cloud DR components in a lockstep manner, upgrading all instances of a given component in all sites.

Upgrade your vCloud Availability for Cloud-to-Cloud DR components in the following order:

- 1 Upgrade all vCloud Availability vApp Replication Service/Manager instances.
- 2 Upgrade all vCloud Availability Replication Manager instances.
- 3 Upgrade all vCloud Availability Replicator instances.
- 4 If you are using Cloud-to-Cloud tunneling, upgrade all vCloud Availability Tunnel instances.

Upgrade vCloud Availability for Cloud-to-Cloud DR by Using the Downloadable ISO Image

You upgrade all vCloud Availability for Cloud-to-Cloud DR components by using a single downloadable ISO image.

Prerequisites

Download the `vCloud-Availability-C2C-1.0.1.XXX-build_number.iso` image from the vCloud Availability for Cloud-to-Cloud DR Download page. Copy the ISO image file to a datastore that is accessible from the vCenter Server instance that you use with vCloud Availability for Cloud-to-Cloud DR.

Procedure

- 1 Mount the ISO file to a vCloud Availability for Cloud-to-Cloud DR appliance.
 - a Log in to the vSphere Web Client on the site where you want to upgrade vCloud Availability for Cloud-to-Cloud DR.
 - b On the home page, click **Hosts and Clusters**.
 - c Right-click the virtual machine that hosts the vCloud Availability for Cloud-to-Cloud DR component that you upgrade and select **Edit Settings**.
 - d On the **Virtual Hardware** tab, select **CD/DVD Drive > Datastore ISO File**.
 - e Follow the prompts to add the CD/DVD drive to the vCloud Availability for Cloud-to-Cloud DR virtual machine and select the **Connected** option.
- 2 Log in to the service management interface for the vCloud Availability for Cloud-to-Cloud DR component that you upgrade using the OS `root` credentials.

You access service management interfaces for vCloud Availability for Cloud-to-Cloud DR in a Web browser, by entering the respective appliance IP address and the port that the service is using. The following table can help you understand which address you need when upgrading the vCloud Availability for Cloud-to-Cloud DR components:

Table 7-1. Services Management Interface Addresses

vCloud Availability for Cloud-to-Cloud DR Component	Management Interface Address and Port
vCloud Availability vApp Replication Service/Manager	<code>https://Appliance-IP-Address:8046</code>
vCloud Availability Replication Manager	<code>https://Appliance-IP-Address:8044</code>
vCloud Availability Replicator	<code>https://Appliance-IP-Address:8043</code>
vCloud Availability Tunnel	<code>https://Appliance-IP-Address:8047</code>

- 3 Navigate to **Update > Settings**, select the **Use CDROM Updates** option, and click **Save Settings**.
- 4 In the **Update** tab, click **Check Updates** and wait for the check to finish.

- 5 Click **Install Updates** and wait for the update to install.

Installing the updates ends your session in the service management interface and you are logged out.

- 6 After the updates install successfully, log in to the service management interface for the vCloud Availability for Cloud-to-Cloud DR component that you upgrade using the OS *root* credentials.
- 7 In the **Diagnostics** tab, click **Reboot VM**.
- 8 Unmount the ISO image.
 - a In the vSphere Web Client, shut down the virtual machine that hosts the vCloud Availability for Cloud-to-Cloud DR component that you upgrade.
 - b Right-click the virtual machine and select **Edit Settings**.
 - c In the **Virtual Hardware** tab, select **CD/DVD Drive** and deselect **Connected** and **Connect At Power On**.
 - d Power on the virtual machine.

vCloud Availability for Cloud-to-Cloud DR Administration

8

Administrative and management tasks occur after you install and configure the vCloud Availability for Cloud-to-Cloud DR solution. They include changes to the provisioned environment and routine administration and maintenance procedures.

This chapter includes the following topics:

- [Add a vCloud Availability Replicator](#)
- [Replace the vCloud Availability vApp Replication Service/Manager Certificate with a CA-Signed Certificate](#)
- [Replace the vCloud Availability Portal Certificate](#)
- [Configure vCloud Availability for Cloud-to-Cloud DR with a Renewed Lookup Service Certificate on a Platform Services Controller](#)
- [Collect vCloud Availability for Cloud-to-Cloud DR Usage Information](#)
- [Collecting Support Bundles for the vCloud Availability for Cloud-to-Cloud DR Components](#)

Add a vCloud Availability Replicator

Depending on your deployment requirements, you can add additional vCloud Availability Replicator instances to your vCloud Availability for Cloud-to-Cloud DR environment.

Prerequisites

Verify that you have configured a vCloud Availability Replicator, a vCloud Availability Replication Manager, and a vCloud Availability vApp Replication Service/Manager instances in your environment.

Procedure

- 1 Add a vCloud Availability Replicator.
 - a In a Web browser, go to `https://Appliance-IP-address:8044`
The *VMware vCloud[®] Replication Manager Getting Started* page opens.
 - b Click **VMware vCloud[®] Availability Replication Manager Configuration Portal**.
 - c Log in with the appliance *root* password that you set during the initial vCloud Availability Replicator configuration.

- d Navigate to **Replicators > New Replicator**.
 - e Select the site to which you add the new vCloud Availability Replicator instance.
 - f (Optional) Add a description for the vCloud Availability Replicator.
 - g In the API URL text box, enter the vCloud Availability vApp Replication Service/Manager address in the following format:

`https://Appliance-IP-address:8043`
 - h Enter the appliance *root* password that you set during the initial vCloud Availability Replicator configuration.
 - i Enter the SSO user name and password.
 - j Click **OK**.
 - k Review the vCloud Availability Replicator certificate details and click **Accept**.
- 2 Re-pair your cloud sites.
- a In a Web browser, go to `https://Appliance-IP-address:8046`.
The *VMware vCloud[®] Availability vApp Replication Manager Server Getting Started* page opens.
 - b Click **VMware vCloud[®] Availability vApp Replication Manager Configuration Portal**.
 - c Log in with the appliance *root* password that you set during the initial vCloud Availability vApp Replication Service/Manager configuration.
 - d Navigate to **Sites > Show all sites**.
 - e To invoke cross-site pairing, click **Repair**.
 - f In the Sites administration pop-up window, enter the vCloud Availability vApp Replication Service/Manager appliance password and click **OK**.

A new vCloud Availability Replicator instance is added to your vCloud Availability for Cloud-to-Cloud DR environment.

Replace the vCloud Availability vApp Replication Service/Manager Certificate with a CA-Signed Certificate

You can optionally configure the vCloud Availability vApp Replication Service/Manager to work with a CA-signed certificate.

The procedure is tested against vCenter Server 6.0.2.

Prerequisites

Make sure that you have the third-party signed certificate and its corresponding private key in a P12-formatted file, for example *custom.p12*.

Procedure

- 1 Log in to the vCloud Availability vApp Replication Service/Manager appliance console as an *administrator*.
- 2 Copy the *custom.p12* archive that contains the externally signed certificate to the /tmp folder of the vCloud Availability vApp Replication Service/Manager appliance.
- 3 Create a backup copy of the certificate that is used by vCloud Availability vApp Replication Service/Manager:

```
$ cp -a /opt/vmware/h4/cloud/config/keystore.jks /opt/vmware/h4/cloud/config/keystore.jks.bak
```

- 4 To retrieve the certificate alias, inspect the *custom.p12* archive:

```
$ keytool -list -v -keystore /tmp/custom.p12
```

- a When prompted, enter the password that protects the *custom.p12* archive.
 - b In the command output, note the alias of the certificate that you want to use for the vCloud Availability vApp Replication Service/Manager appliance.
- 5 Import the new keystore to the vCloud Availability vApp Replication Service/Manager keystore:

```
$ keytool -importkeystore -srckeystore /tmp/custom.p12 -srcstoretype pkcs12 -srcalias certificate_alias -destkeystore /opt/vmware/h4/cloud/config/keystore.jks \
-deststoretype jks -deststorepass vmware -destalias cloud
```

- a When prompted for a password, enter the password that protects the *custom.p12* archive.
 - b When prompted to override the currently used certificate with the new one, enter **Yes** and press Enter.
- 6 Update the communication settings between services in the vCloud Availability vApp Replication Service/Manager appliance.

```
$ /opt/vmware/h4/bin/sysboot.py
```

- 7 Restart the vCloud Availability vApp Replication Service/Manager services:

```
$ systemctl restart cloud
```

- 8 Configure the vCloud Availability Portal to use the new vCloud Availability vApp Replication Service/Manager certificate.
 - a In a Web browser, navigate to the vCloud Configuration Portal at `https://Appliance-IP-Address:5480`.
 - b Log in as an administrator.
 - c In the vApp RM tab, click **Edit**.

- d Enter SSO user name and password.
 - e Click **Connect**.
- 9 Repair your cloud sites.
- a In a Web Browser, navigate to the vCloud Availability vApp Replication Service/Manager Configuration Portal at `https://Appliance-IP-Address:8046`.
The *VMware vCloud[®] Availability vApp Replication Manager Server Getting Started* page opens.
 - b Click **VMware vCloud[®] Availability vApp Replication Manager Configuration Portal**.
 - c Log in as an administrator.
 - d Navigate to **Sites > Show all sites**.
 - e Click **Repair**.
A pop-up window appears.
 - f Enter the vCloud Availability vApp Replication Service/Manager appliance password and click **OK**.

The vCloud Availability vApp Replication Service/Manager appliance is set to use the CA-signed certificate. You can revert to the previously used certificate by running the following command in the appliance console:

```
$ cp -a /opt/vmware/h4/cloud/config/keystore.jks.bak /opt/vmware/h4/cloud/config/keystore.jks &&  
touch /opt/vmware/h4/cloud/config/keystore.jks && systemctl restart cloud
```

Replace the vCloud Availability Portal Certificate

To replace the vCloud Availability Portal certificate, you generate a new certificate, or import a third-party certificate by using the vCloud Configuration Portal.

Prerequisites

Verify that a vCloud Availability Portal is configured. For more information, see [Configure a vCloud Availability Portal](#).

Procedure

- 1 In a Web browser, go to the vCloud Configuration Portal at `https://Appliance-IP-Address:5480`.
- 2 Log in using the appliance *root* password.
- 3 Navigate to **Portal Service > Certificate**.
The details of the currently used vCloud Availability Portal certificate are displayed.
- 4 Click **Replace**.
A *Replace Certificate* pop-up window opens.

5 Replace the vCloud Availability Portal certificate.

Note If you are using a third-party certificate, make sure that the certificate .pem file contains both a private key and certificate.

Option	Description
Auto Generate	To generate a new SSL certificate for vCloud Availability Portal, click Auto Generate .
Upload	To upload a third-party certificate, click Upload and select the certificate .pem file.
Certificate Panel	You can also copy the content of the certificate .pem file and paste it in the <i>Certificate Panel</i> .

6 Click **Submit**.

A *Certificate replaced successfully* message appears.

Replacing the vCloud Configuration Portal certificate triggers a restart of the vCloud Availability Portal Service.

Configure vCloud Availability for Cloud-to-Cloud DR with a Renewed Lookup Service Certificate on a Platform Services Controller

If you renew the Lookup Service certificate on a Platform Services Controller (PSC), you must configure vCloud Availability for Cloud-to-Cloud DR components to work with the new certificate.

Prerequisites

- Make sure that you have successfully renewed the PSC certificate and that the Lookup Service is updated with the new certificate. For more information, see <https://kb.vmware.com/s/article/2118939>.
- Make sure that all components in your environment that rely on the vCenter Server registration in the Lookup Service are configured to accept the new certificate. An example of such a component is NSX Manager.

Procedure

1 Configure the vCloud Availability Replicator to work with the new PSC certificate.

If you are not using the Combined deployment type and have dedicated vCloud Availability Replicator appliances, repeat the step for every vCloud Availability Replicator instance.

- a In a Web Browser, navigate to the vCloud Availability Replicator Configuration Portal at `https://Appliance-IP-Address:8043`.

The *VMware vCloud[®] Availability Replicator Server Getting Started* page opens.

- b Click **VMware vCloud[®] Availability Replicator Configuration Portal**.
- c Log in with the *root* password of the appliance.

- d In the Configuration tab, click **Set lookup service**.
 - e Enter the Lookup Service address and click **OK**.
The details of the new certificate appear.
 - f Review and accept the new Lookup Service certificate.
- 2 Configure the vCloud Availability Replication Manager to work with the new PSC certificate.
- a In a Web Browser, navigate to the vCloud Availability Replication Manager Configuration Portal at `https://Appliance-IP-Address:8044`.
The *VMware vCloud[®] Replication Manager Getting Started* page opens.
 - b Click **VMware vCloud[®] Availability Replication Manager Configuration Portal**.
 - c Log in with the *root* password of the appliance.
 - d In the Configuration tab, click **Set lookup service**.
 - e Enter the Lookup Service address and click **OK**.
The details of the new certificate appear.
 - f Review and accept the new Lookup Service certificate.
- 3 Configure the vCloud Availability vApp Replication Service/Manager to work with the new PSC certificate.
- a In a Web Browser, navigate to the vCloud Availability vApp Replication Service/Manager Configuration Portal at `https://Appliance-IP-Address:8046`.
The *VMware vCloud[®] Availability vApp Replication Manager Server Getting Started* page opens.
 - b Click **VMware vCloud[®] Availability vApp Replication Manager Configuration Portal**.
 - c Log in with the *root* password of the appliance .
 - d In the Configuration tab, click **Set lookup service**.
 - e Enter the Lookup Service address and click **OK**.
The details of the new certificate appear.
 - f Review and accept the new Lookup Service certificate.
- 4 Restart the replicator service for all vCloud Availability Replicator instances in the same site.
- If you are not using the Combined deployment type and have dedicated vCloud Availability Replicator appliances, repeat the step for every vCloud Availability Replicator instance.
- a In the vCloud Availability Replicator Configuration Portal, navigate to **Diagnostics > Health**.
 - b Click **Reboot Services**.
 - c Confirm the reboot by clicking **Reboot** in the pop-up message.

Collect vCloud Availability for Cloud-to-Cloud DR Usage Information

This procedure outlines extracting usage information from your vCloud Availability for Cloud-to-Cloud DR installation. You can use the exported information for reporting purposes.

Procedure

- 1 Log in to the vCloud Availability vApp Replication Service/Manager appliance console as *root*.

```
$ c4 loginroot C4-Root-Password
```

- 2 (Optional) To verify that the usage report generates properly, run the following command.

```
$ usage-report
```

The system returns the vCloud Availability for Cloud-to-Cloud DR in the following format:

```
# vCloud Availability C2C DR Usage Report

generatedOn 2018-05-14 13:18:47.634510
productName vSphere Replication Cloud (C4)
buildVersion 1.1.0.2623-70917fa
localSite site2
instanceId 7c6198d8-e608-4396-be7e-defc29abdab7

Total incoming vApp replications      2
Total incoming VM replications        3

Incoming vApp replications by org
Org Org Id Number of Replications
AnotherOrg 980ce8bc-afc0-402e-9bf3-f0fb51d9ed4d 1
s2Org 4031acf0-a702-4652-8de2-fc2af2ab7e2e 1

Incoming VM replications by org
Org Org Id Number of Replications
AnotherOrg 980ce8bc-afc0-402e-9bf3-f0fb51d9ed4d 2
s2Org 4031acf0-a702-4652-8de2-fc2af2ab7e2e 1

Incoming vApp replications by vDC
vDC vDC Id Org Number of Replications
AnotherVdc c14e2678-28c8-47d0-bf5b-69043074533f AnotherOrg 1
vdc_s2Org 38338c25-eb91-4607-9328-7faf8cde69b7 s2Org 1

Incoming VM replications by vDC
vDC vDC Id Org Number of Replications
AnotherVdc c14e2678-28c8-47d0-bf5b-69043074533f AnotherOrg 2
vdc_s2Org 38338c25-eb91-4607-9328-7faf8cde69b7 s2Org 1

# End of report.
```

- 3 (Optional) Retrieve more information about the `usage-report` script.

```
$ usage-report --help
```

- 4 Generate the vCloud Availability for Cloud-to-Cloud DR usage report.

```
$ usage-report --output /tmp/report_summary.tsv --details /tmp/report_details.tsv
```

The vCloud Availability for Cloud-to-Cloud DR usage report consists of two `.tsv` files.

The `/tmp/report_summary.tsv` file contains information about the total incoming replications and information about incoming replications aggregated by Organizations and by vDC.

The `/tmp/report_details.tsv` file contains information about individual incoming replications.

- 5 Download the vCloud Availability for Cloud-to-Cloud DR usage report locally.

```
$ scp /tmp/report_summary.tsv /tmp/report_details.tsv user@your-host:/download-target-location
```

- 6 (Optional) Remove the generated reports from the vCloud Availability vApp Replication Service/Manager appliance.

```
$ rm /tmp/report_summary.tsv /tmp/report_details.tsv
```

What to do next

You generated the vCloud Availability for Cloud-to-Cloud DR usage report and, for example, you can aggregate the information to report to the VMware Cloud Provider Program.

Collecting Support Bundles for the vCloud Availability for Cloud-to-Cloud DR Components

VMware Technical Support routinely requests diagnostic information from you when a support request is handled. The information is gathered using a specific script or tool for each product. Support bundles contain product-specific logs, configuration files, and data appropriate to the situation.

Collecting a Support Bundle from vCenter Server

You can generate the vCenter Server support bundle by performing the following steps:

- 1 In a Web browser, navigate to `https://(vCenter_Server_FQDN):443/appliance/support-bundle`.
- 2 Enter root credentials and click **Enter**.
- 3 The download starts.

For more information about vCenter Server Diagnostic, see [Collecting diagnostic information for VMware vCenter Server KB Article](#).

Collecting a Support Bundle from vCloud Director

To collect the vCloud Director support bundle, establish an SSH connection to **one** of the vCloud Director VMs and run the following command:

```
/opt/vmware/vcloud-director/bin/vmware-vcd-support --all --multicell
```

The command produces a file in the following format: `vmware-cvd-support-YYYY-MM-DD.NNNN.tgz`. The support bundle file is at: `/opt/vmware/vcloud-director/data/transfer/vmware-vcd-support`

Collecting a Support Bundle from vCloud Availability Replication Manager

To collect the support bundle for vCloud Availability Replication Manager, perform the following steps:

- 1 In a Web browser, go to `https://Appliance-IP-address:8044`.
The *VMware vCloud[®] Replication Manager Getting Started* page opens.
- 2 Click **VMware vCloud[®] Availability Replication Manager Configuration Portal**.
You are redirected to the Replication Manager Configuration Portal login page.
- 3 Log in with the appliance *root* password that you set during the initial vCloud Availability Replicator configuration.
You are redirected to the vCloud Availability Replication Manager health status page.
- 4 Navigate to **Diagnostics > Support Bundles**.
- 5 Click **Generate New Bundle**.
A pop-up window indicating the process progress appears.
- 6 After the bundle is generated, to save the support bundle file locally, click **Download**.

The vCloud Availability Replication Manager support bundle includes support bundles from all connected vCloud Availability Replicator instances.

Collecting a Support Bundle from vCloud Availability Replicator

To collect the support bundle for vCloud Availability Replicator, perform the following steps:

- 1 In a Web browser, go to `https://Appliance-IP-address:8043`.
The *VMware vCloud[®] Availability Replicator Server Getting Started* page opens.
- 2 Click **VMware vCloud[®] Availability Replicator Configuration Portal**.
You are redirected to the Replicator Configuration Portal page.
- 3 Log in as *root*.
You are redirected to the vCloud Availability Replicator health status page.

- 4 Navigate to **Diagnostics > Support Bundles**.
- 5 Click **Generate New Bundle**.
A pop-up window indicating the process progress appears.
- 6 After the bundle is generated, to save the support bundle file locally, click **Download**.

Collecting a Support Bundle from vCloud Availability vApp Replication Service/Manager

To collect the support bundle for vCloud Availability vApp Replication Service/Manager, perform the following steps:

- 1 In a Web browser, go to `https://Appliance-IP-address:8046`.
The *VMware vCloud[®] Availability vApp Replication Manager Server Getting Started* page opens.
- 2 Click **VMware vCloud[®] Availability vApp Replication Manager Configuration Portal**.
You are redirected to the vCloud Availability vApp Replication Manager Configuration Portal login page.
- 3 Log in as *root*.
You are redirected to the vCloud Availability vApp Replication Service/Manager health status page.
- 4 Navigate to **Diagnostics > Support Bundles**.
- 5 Click **Generate New Bundle**.
A pop-up window indicating the process progress appears.
- 6 After the bundle is generated, to save the support bundle file locally, click **Download**.