

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

11 OCT 2018

VMware vCloud Availability 1.5



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 © 2019 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 Overview of vCloud Availability for Cloud-to-Cloud DR** 8
 - [vCloud Availability for Cloud-to-Cloud DR Services](#) 10
 - [vCloud Availability for Cloud-to-Cloud DR Services Requirements](#) 12
 - [vCloud Availability for Cloud-to-Cloud DR Network Port Configuration](#) 14
- 3 vCloud Availability for Cloud-to-Cloud DR Deployment Requirements** 18
- 4 Deploy vCloud Availability for Cloud-to-Cloud DR Services Using the vSphere Web Client** 20
- 5 Deploying vCloud Availability for Cloud-to-Cloud DR Services with OVF Tool** 23
 - [Defining OVF Tool Parameters for vCloud Availability for Cloud-to-Cloud DR Services Deployment](#) 23
 - [Deploy vCloud Availability for Cloud-to-Cloud DR Services Using the OVF Tool](#) 24
- 6 Configuring vCloud Availability for Cloud-to-Cloud DR Services** 27
 - [Initial vCloud Availability for Cloud-to-Cloud DR Services Configuration](#) 27
 - [Configure a vCloud Availability Replicator](#) 27
 - [Configure a vCloud Availability Replication Manager](#) 28
 - [Configure a vCloud Availability vApp Replication Manager](#) 29
 - [Register a vCloud Availability Replicator with a vCloud Availability Replication Manager in the Same Site](#) 31
 - [Configuring Cloud-to-Cloud Tunneling](#) 32
 - [Configure Cloud-to-Cloud Tunneling by Using the vCloud Availability Tunnel Command-Line Interface](#) 33
 - [Configure Cloud-to-Cloud Tunneling by Using the vCloud Availability for Cloud-to-Cloud DR Portal](#) 36
 - [Pair Cloud Sites](#) 38
- 7 Configuring the Customer Experience Improvement Program** 40
 - [Categories of Information That VMware Receives](#) 40
 - [Join or Leave the Customer Experience Improvement Program](#) 40

- 8 Upgrading vCloud Availability for Cloud-to-Cloud DR 41**
 - Order of Upgrading vCloud Availability for Cloud-to-Cloud DR Components 42
 - Upgrade vCloud Availability for Cloud-to-Cloud DR Components by Using the Default VMware Repository 42
 - Upgrade vCloud Availability for Cloud-to-Cloud DR by Using an ISO Image 43
 - Upgrade vCloud Availability for Cloud-to-Cloud DR Components by Using a Specified Repository 44
 - Install the vCloud Availability for Cloud-to-Cloud DR Plug-In for vCloud Director 46
 - Start Working with vCloud Availability for Cloud-to-Cloud DR 1.5 47

- 9 Managing vCloud Availability for Cloud-to-Cloud DR 49**
 - Add a New vCloud Availability Replicator 49
 - Reestablish Cloud Sites Trust 51
 - Certificate Management in vCloud Availability for Cloud-to-Cloud DR 51
 - Configure vCloud Availability for Cloud-to-Cloud DR with a Renewed Lookup Service Certificate on a Platform Services Controller 51
 - Replace the vCloud Availability vApp Replication Manager Certificate with a CA-Signed Certificate 53
 - Renew the SSL Certificate of the vCloud Availability Replicator Service 54
 - Renew the SSL Certificate of the vCloud Availability Replication Manager Service 56
 - Renew the SSL Certificate of the vCloud Availability vApp Replication Manager Service 57
 - Collect vCloud Availability for Cloud-to-Cloud DR Usage Information 58
 - Collect vCloud Availability for Cloud-to-Cloud DR Storage Consumption Information 60
 - Troubleshooting vCloud Availability for Cloud-to-Cloud DR 62
 - Set or Update a Network Time Protocol Configuration 62
 - Cannot Access vCloud Availability for Cloud-to-Cloud DR Portal Through vCloud Director 63
 - Collecting Support Bundles for the vCloud Availability for Cloud-to-Cloud DR Components 64

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, upgrade, and administer 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 Scripting

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
6 DEC 2018	<p>Removed the following topics:</p> <ul style="list-style-type: none"> ■ <i>Pairing Cloud Sites</i> ■ <i>Pair Cloud Sites When Cloud-to-Cloud Tunneling Is Configured</i> ■ <i>Reestablishing Trust Between Cloud Sites</i> ■ <i>Reestablish Cloud Sites Trust When Cloud-to-Cloud Tunneling Is Configured</i> <p>Updated the information in the following topics:</p> <ul style="list-style-type: none"> ■ Pair Cloud Sites ■ Start Working with vCloud Availability for Cloud-to-Cloud DR 1.5 ■ Reestablish Cloud Sites Trust ■ Add a New vCloud Availability Replicator ■ Replace the vCloud Availability vApp Replication Manager Certificate with a CA-Signed Certificate ■ Renew the SSL Certificate of the vCloud Availability Replicator Service ■ Renew the SSL Certificate of the vCloud Availability Replication Manager Service ■ Renew the SSL Certificate of the vCloud Availability vApp Replication Manager Service
14 NOV 2018	<p>Added the following topics:</p> <ul style="list-style-type: none"> ■ Chapter 5 Deploying vCloud Availability for Cloud-to-Cloud DR Services with OVF Tool ■ Defining OVF Tool Parameters for vCloud Availability for Cloud-to-Cloud DR Services Deployment ■ Install the vCloud Availability for Cloud-to-Cloud DR Plug-In for vCloud Director ■ Certificate Management in vCloud Availability for Cloud-to-Cloud DR ■ Renew the SSL Certificate of the vCloud Availability Replicator Service ■ Renew the SSL Certificate of the vCloud Availability Replication Manager Service ■ Renew the SSL Certificate of the vCloud Availability vApp Replication Manager Service ■ Troubleshooting vCloud Availability for Cloud-to-Cloud DR ■ Set or Update a Network Time Protocol Configuration ■ Cannot Access vCloud Availability for Cloud-to-Cloud DR Portal Through vCloud Director <p>Updated the information in the following topics:</p> <ul style="list-style-type: none"> ■ Chapter 3 vCloud Availability for Cloud-to-Cloud DR Deployment Requirements ■ Chapter 4 Deploy vCloud Availability for Cloud-to-Cloud DR Services Using the vSphere Web Client ■ Deploy vCloud Availability for Cloud-to-Cloud DR Services Using the OVF Tool ■ Configure a vCloud Availability Replication Manager ■ Configure Cloud-to-Cloud Tunneling by Using the vCloud Availability Tunnel Command-Line Interface ■ Configure Cloud-to-Cloud Tunneling by Using the vCloud Availability for Cloud-to-Cloud DR Portal ■ Chapter 9 Managing vCloud Availability for Cloud-to-Cloud DR
16 OCT 2018	<p>Added the Reestablish Cloud Sites Trust topic.</p> <p>Updated the information in the following topics:</p> <ul style="list-style-type: none"> ■ Chapter 4 Deploy vCloud Availability for Cloud-to-Cloud DR Services Using the vSphere Web Client ■ Pair Cloud Sites ■ Start Working with vCloud Availability for Cloud-to-Cloud DR 1.5 ■ Replace the vCloud Availability vApp Replication Manager Certificate with a CA-Signed Certificate
11 OCT 2018	Initial release.

Overview of vCloud Availability for Cloud-to- Cloud DR

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.

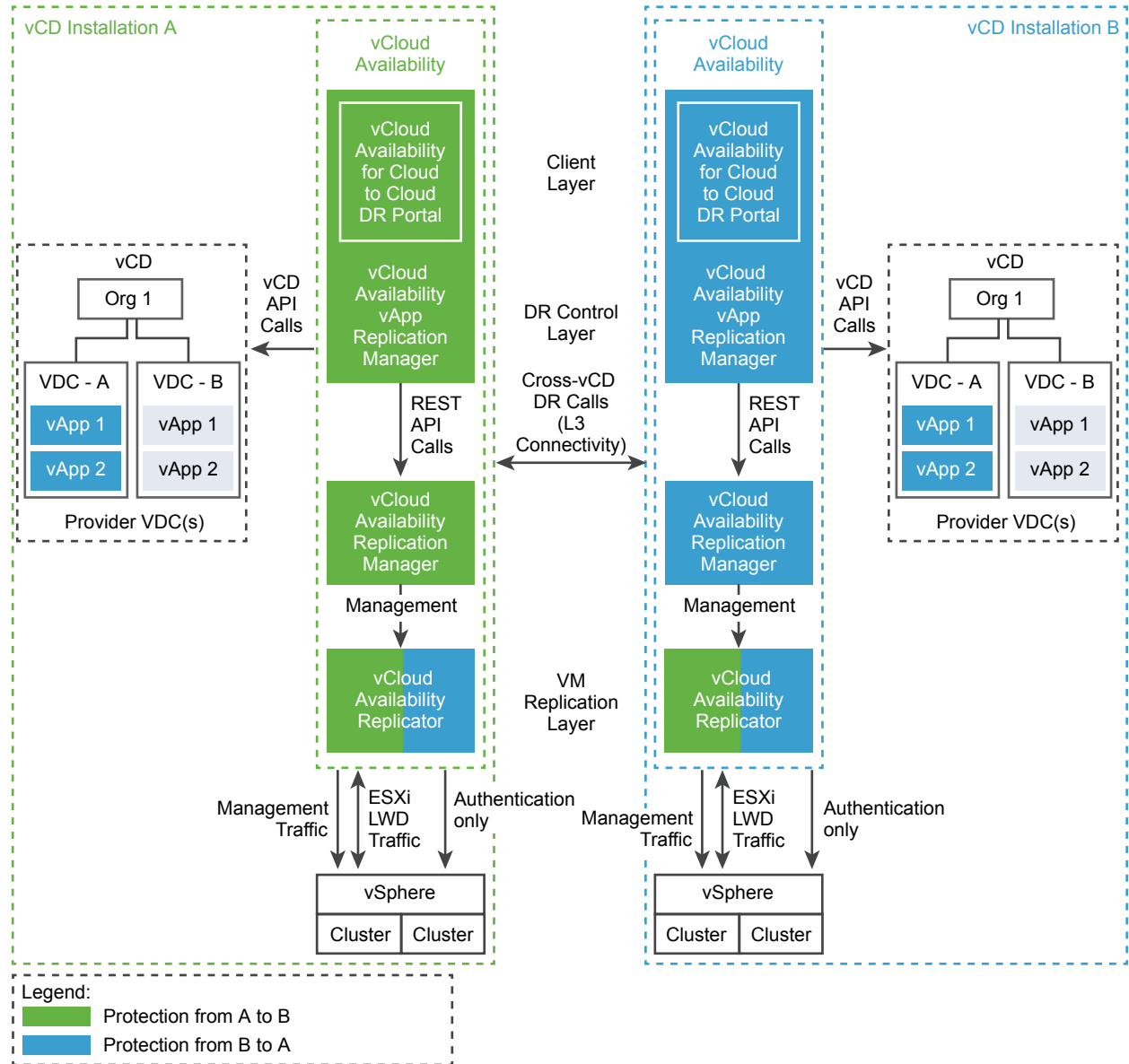
The service operates through a VMware Cloud Provider Program, and each installation provides recovery for multiple cloud environments. The vCloud Availability for Cloud-to-Cloud DR provides:

- 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.
- Using a single-site vCloud Availability for Cloud-to-Cloud DR installation, you can migrate vApps and VMs between Virtual Data Centers that belong to a single vCloud Director Organization.
- Secure Tunneling through a 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.

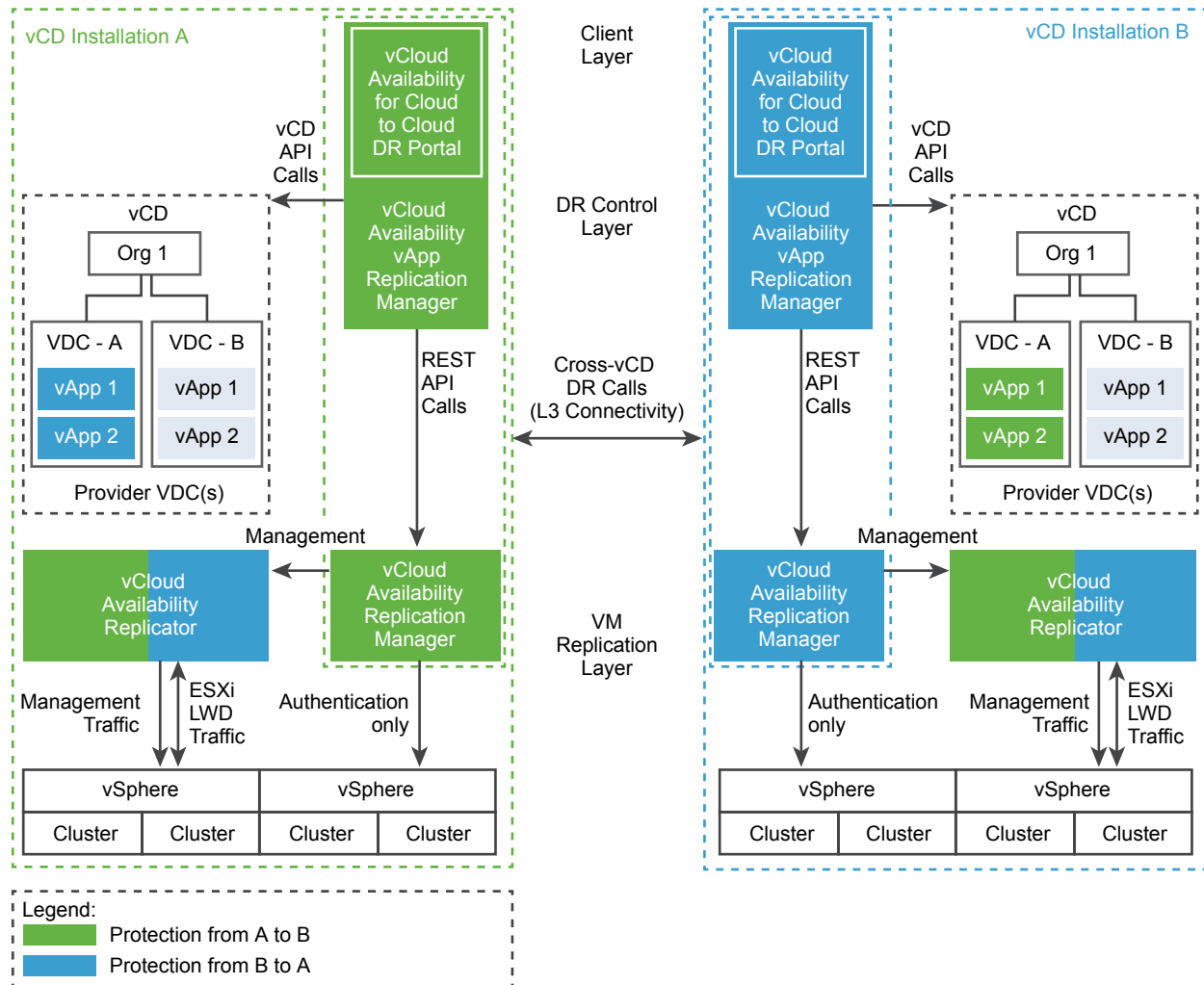
The architecture of the solution relies on symmetrical replication operations between cloud environments. In a single cloud environment, the vCloud Availability Replicator, the vCloud Availability Replication Manager, and the vCloud Availability vApp Replication Manager operate together to support the 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.

The components with no color in the following diagrams 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.



For production deployments, you deploy and configure a single appliance that hosts the vCloud Availability for Cloud-to-Cloud DR portal, vCloud Availability vApp Replication Manager, and vCloud Availability Replication Manager services. You deploy and configure dedicated vCloud Availability Replicator appliance or appliances.



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 composed of services that 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 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.
Lightweight Delta Protocol Service(LWD Proxy)	The proprietary replication protocol service 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 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.

The vCloud Availability for Cloud-to-Cloud DR services provide a management interface for configuration and administration purposes.

You perform initial configuration of vCloud Availability for Cloud-to-Cloud DR services by using the vCloud Availability Replication Manager, vCloud Availability Replicator, and vCloud Availability vApp Replication Manager management interfaces.

You cannot access the vCloud Availability for Cloud-to-Cloud DR portal before finishing the initial vCloud Availability for Cloud-to-Cloud DR configuration.

The following table lists the services management interface addresses of vCloud Availability for Cloud-to-Cloud DR services.

Table 2-2. Services Management Interface Addresses

vCloud Availability for Cloud-to-Cloud DR Component	Management Interface Address and Port
vCloud Availability vApp Replication Manager	https://Appliance-IP-Address:8046/ui/admin
vCloud Availability Replication Manager	https://Appliance-IP-Address:8044/ui/admin

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

vCloud Availability for Cloud-to-Cloud DR Component	Management Interface Address and Port
vCloud Availability Replicator	https://Appliance-IP-Address:8043/ui/admin
vCloud Availability Tunnel	https://Appliance-IP-Address:8047/ui/admin

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 Manager	/opt/vmware/h4/cloud/config/application.properties
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 Manager	/opt/vmware/h4/cloud/log/cloud.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 Manager Users Requirements

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

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

vCloud Availability for Cloud-to-Cloud DR User Sessions Requirements

Each vCloud Availability for Cloud-to-Cloud DR user session is guaranteed to have a vCloud Director user and vCloud Director organization associated with the session.

To manage vCloud Availability for Cloud-to-Cloud DR objects and the local vCloud Availability vApp Replication Manager appliance as a service provider, you start a user session as a vCloud Director **system administrator** by using vCloud Director user name and password. **System administrator** users can manage any local and monitor any remote vCloud Availability for Cloud-to-Cloud DR inventory object. To manage vCloud Availability for Cloud-to-Cloud DR objects in the remote sites, you must authenticate as a system administrator to the remote site.

To perform disaster recovery operations and manage local vCloud Availability for Cloud-to-Cloud DR objects as a tenant user, you start a user session as a vCloud Director organization administrator by using vCloud Director credentials. As an organization administrator, you can perform disaster recovery operations in the local site, you can manage any local vCloud Availability for Cloud-to-Cloud DR object, and can monitor any remote vCloud Availability for Cloud-to-Cloud DR object that belongs to the respective vCloud Director organization. To manage remote vCloud Availability for Cloud-to-Cloud DR objects, you must authenticate to the corresponding remote organization.

For more information about authenticating to remote sites, see the *Authenticate to Remote Sites as a Service Provider* and *Authenticate to Remote Sites as a Tenant* topics in *vCloud Availability for Cloud-to-Cloud DR User's Guide*.

The following table lists vCloud Availability vApp Replication Manager disaster recovery operations that require sessions on either of the sites, or both.

Table 2-5. vCloud Availability vApp Replication 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 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 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 instances within a vCloud Director site must be within the same single sign-on domain. All vCloud Availability Replicator, vCloud Availability Replication Manager, and vCloud Availability vApp Replication Manager appliances within the respective site must be configured with that same single sign-on 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 configured 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	HTTPS	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.	443	HTTPS	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 Manager service or vCloud Availability Replicator service	All PSCs	7444	TCP	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 Manager Service or vCloud Availability Replicator Service	Local vCenter Server	443	HTTPS	Used by the local vCloud Availability vApp Replication Manager service or the vCloud Availability Replicator service for communication with the local vCenter Server.
vCloud Availability Replicator service	Local ESXi hosts	902	TCP and UDP	Used by the vCloud Availability Replicator service for replication traffic to the destination ESXi hosts.
Local ESXi hosts	Local LWD Proxy service	44046	LWD	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 communication.

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 Manager service	8443	HTTPS	The vCloud Availability vApp Replication 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 Manager service in the source site	vCloud Availability vApp Replication Manager service in the destination site	8046	HTTPS	Used for vCloud Availability vApp Replication Manager management from a source site to a local vCloud Availability vApp Replication Manager service.

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

Source	Destination	Port Number	Protocol	Description
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	HTTPS	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.	443	HTTPS	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 Manager service or vCloud Availability Replicator service	All PSCs	7444	TCP	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 Manager service or vCloud Availability Replicator service	Local vCenter Server	443	TCP	Used by the local vCloud Availability vApp Replication Manager service or the vCloud Availability Replicator service for communication with the local vCenter Server.
vCloud Availability Replicator service	Local ESXi hosts	902	TCP and UDP	Used by the vCloud Availability Replicator service for replication traffic to the destination ESXi hosts.
Local ESXi hosts	Local LWD Proxy service	44046	LWD	Used for replication data traffic from a protected ESXi host to the local LWD Proxy.

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

Source	Destination	Port Number	Protocol	Description
vCloud Availability Tunnel appliance	Local LWD Proxy service	44045	LWDS	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 Manager service	8046	HTTPS	vCloud Availability vApp Replication Manager service management from the vCloud Availability Tunnel appliance.
vCloud Availability Tunnel appliance	vCloud Availability Replicator service	8043	HTTPS	vCloud Availability Replicator management from the vCloud Availability Tunnel.
vCloud Availability Tunnel	vCloud Availability Replication Manager	8044	HTTPS	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 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.

Deployment Types and Hardware Requirements

You install 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.

Depending on your scale and deployment goals, you can select various deployment types. The following table describes the different deployment types and hardware requirements.

Table 3-1. vCloud Availability for Cloud-to-Cloud DR Deployment Types

Deployment Type	Description	Hardware Requirements
Combined	<p>All-in-one deployment type that is suitable for testing, evaluation, and small-scale environments. Includes the following services:</p> <ul style="list-style-type: none"> vCloud Availability Replication Manager vCloud Availability Replicator vCloud Availability vApp Replication Manager vCloud Availability for Cloud-to-Cloud DR portal <p>You deploy a single appliance with all vCloud Availability for Cloud-to-Cloud DR services ready for configuration.</p>	<ul style="list-style-type: none"> 4 vCPUs 6 GB RAM 10 GB Storage
Manager node	<p>Deploys a single appliance that contains the following services:</p> <ul style="list-style-type: none"> vCloud Availability Replication Manager vCloud Availability vApp Replication Manager vCloud Availability for Cloud-to-Cloud DR portal 	<ul style="list-style-type: none"> 4 vCPUs 4 GB RAM 10 GB Storage
Replicator Node	<p>Deploys a dedicated vCloud Availability Replicator appliance.</p>	<ul style="list-style-type: none"> 2 vCPUs 4 GB RAM 10 GB Storage

Table 3-1. vCloud Availability for Cloud-to-Cloud DR Deployment Types (Continued)

Deployment Type	Description	Hardware Requirements
Large Replicator	Deploys a dedicated vCloud Availability Replicator appliance suitable for large-scale environments.	<ul style="list-style-type: none"> ■ 4 vCPUs ■ 6 GB RAM ■ 10 GB Storage
Tunnel Node	Deploys a vCloud Availability Tunnel appliance suitable for small-scale environments.	<ul style="list-style-type: none"> ■ 2 vCPUs ■ 2 GB RAM ■ 10 GB Storage

Other Deployment 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 the 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*.
- You deploy a vCloud Availability vApp Replication Manager in two sites, for example *site1* and *site2*. Each of the sites consists of a vCloud Director installation, for example vCD and a resource vCenter Server with at least one ESXi host.
- 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 Using the vSphere Web Client

4

You install 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.

Prerequisites

- Download the installation `vCloud-Availability-C2C-release_number-xxx-build_number_OVF10.ova` file that contains all vCloud Availability for Cloud-to-Cloud DR appliances binaries.
- Verify that you installed the Client Integration Plug-in so that you can use the `Deploy OVF Template` option in the vSphere Web Client.

Procedure

- 1 Log in to the vSphere Web Client.
- 2 Right-click the target location, for example data center, folder, cluster, resource pool, or host, where you want to deploy the vCloud Availability for Cloud-to-Cloud DR services.
- 3 From the drop-down menu, select `Deploy OVF Template`.

The **Deploy OVF Template** wizard opens.

- 4 In the **Select source** page, browse to the `vCloud-Availability-C2C-release_number-xxx-build_number_OVF10.ova` file location and click **Next**.
- 5 Review the OVF template details and click **Next**.
- 6 Accept the terms in the license agreement and click **Next**.
- 7 Enter a name for the deployed appliance.
- 8 Select a data center, or data center folder that contains the host, or cluster on which you want to deploy the appliance, and click **Next**.
- 9 Select a deployment type and click **Next**.

The following table describes the types of deployment for vCloud Availability for Cloud-to-Cloud DR services.

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

Deployment Type	Description
Combined	<p>All-in-one deployment type that is suitable for testing, evaluation, and small-scale environments. Includes the following services:</p> <ul style="list-style-type: none"> ■ vCloud Availability Replication Manager ■ vCloud Availability Replicator ■ vCloud Availability vApp Replication Manager ■ vCloud Availability for Cloud-to-Cloud DR portal <p>You deploy a single appliance with all vCloud Availability for Cloud-to-Cloud DR services ready for configuration.</p>
Manager node with vCloud Director	<p>Deploys a single appliance that contains the following services:</p> <ul style="list-style-type: none"> ■ vCloud Availability Replication Manager ■ vCloud Availability vApp Replication Manager ■ vCloud Availability for Cloud-to-Cloud DR portal
Replicator Node	Deploys a dedicated vCloud Availability Replicator appliance.
Large Replicator Node	Deploys a dedicated vCloud Availability Replicator appliance suitable for large-scale environments.
Tunnel Node	Deploys a vCloud Availability Tunnel appliance suitable for small-scale environments.

- 10 Select a host, or cluster as a destination on which you want the appliance to run, and click **Next**.
- 11 Select the virtual disk format and the storage policy for the appliance from the drop-down menu.
- 12 (Optional) Configure the network settings and click **Next**.
- 13 Customize the deployment properties of the vCloud Availability for Cloud-to-Cloud DR appliance and click **Next**.
 - a 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 Enter and confirm the password for the **root** user for the appliance.

The default password is **vmware**. If you leave the **root** password section empty, the default password is set for the **root** user. You can use this password only once and must change the **root** user password after you log in for the first time.
- 14 (Optional) Review all the settings and select **Power on after deployment**.
- 15 To begin the OVA installation process, click **Finish**.

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

What to do next

If you did not select the Enable SSH option during deployment, you can reconfigure the appliance. For more information, see <https://kb.vmware.com/s/article/59197>.

Deploying vCloud Availability for Cloud-to- Cloud DR Services with OVF Tool

5

To deploy vCloud Availability for Cloud-to-Cloud DR services by using the VMware OVF Tool, define deployment parameters and run a deployment script.

This chapter includes the following topics:

- [Defining OVF Tool Parameters for vCloud Availability for Cloud-to-Cloud DR Services Deployment](#)
- [Deploy vCloud Availability for Cloud-to-Cloud DR Services Using the OVF Tool](#)

Defining OVF Tool Parameters for vCloud Availability for Cloud-to-Cloud DR Services Deployment

Before you deploy vCloud Availability for Cloud-to-Cloud DR services, you must define the specific OVF Tool parameters for deployment.

The following table describes the parameters you must define when deploying vCloud Availability for Cloud-to-Cloud DR services by using the OVF Tool scripts.

Parameter	Description
OVA	The local client path to the installation OVA package. For example, OVA="local_client_path/vCloud-Availability-C2C-release_number-xxx-build_number_OVF10.ova".
VMNAME	Virtual machine name.
VSPHERE_DATASTORE	The VSPHERE_DATASTORE value is the datastore name as it is displayed in the vSphere Web Client.
VSPHERE_NETWORK	The name of the network on which the appliance to run.
VCENTER_SERVER_ADDRES S	The IP address of the vCenter Server instance on which you deploy the appliance.

Parameter	Description
VCENTER_SERVER_USER	User name for a vCenter Server administrator.
VSPHERE_LOCATOR	<p>The VSPHERE_LOCATOR value contains the target data center name, the tag <i>host</i>, 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.</p> <ul style="list-style-type: none"> ▪ <i>/data-center-name/host/cluster-1-name/ESXi-host-fully-qualified-domain-name</i> ▪ <i>/data-center-name/host/cluster-2-name/ESXi-host-IP-address</i> <p>If the target ESXi host is not part of a cluster, skip the <i>cluster-name</i> element, as shown in the following examples.</p> <ul style="list-style-type: none"> ▪ <i>/data-center-name/host/ESXi-host-fully-qualified-domain-name</i> ▪ <i>/data-center-name/host/ESXi-host-IP-address</i> <p>For more information about the VSPHERE_LOCATOR value, run the <code>./ovftool --help locators</code> command.</p>

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

To deploy vCloud Availability for Cloud-to-Cloud DR services, define deployment parameters in your OVF Tool user session, and run the deployment script.

You install 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.

Prerequisites

- Download the installation `vCloud-Availability-C2C-release_number-xxx-build_number_OVF10.ova` file that contains all vCloud Availability for Cloud-to-Cloud DR appliances binaries.
- Verify that you have the OVF Tool installed and configured.

Procedure

- 1 Open an SSH session to the server where the OVF Tool is installed and configured.
- 2 Define deployment parameters in the OVF Tool console by running the following commands.

```
# 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=vCenter-Server-ip-address
```



```
# VSPHERE_USER=vCenter-Server-admin-user

# VSPHERE_LOCATOR="vsphere-locator"
```

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

The value you set for the `--deploymentOption` argument controls the deployment type for the appliance you deploy. The following table lists the deployment types and the corresponding values for the OVF Tool `--deploymentOption` argument.

Table 5-1. vCloud Availability for Cloud-to-Cloud DR Deployment Types and OVF Tool Deployment Options

Deployment types	OVF Tool Deployment Option	Description
Combined	combined	All-in-one deployment type that is suitable for testing, evaluation, and small-scale environments. Includes the following services: <ul style="list-style-type: none"> ■ vCloud Availability Replication Manager ■ vCloud Availability Replicator ■ vCloud Availability vApp Replication Manager ■ vCloud Availability for Cloud-to-Cloud DR portal You deploy a single appliance with all vCloud Availability for Cloud-to-Cloud DR services ready for configuration.
Manager Node with vCloud Director Support	cloud	Deploys a single appliance that contains the following services: <ul style="list-style-type: none"> ■ vCloud Availability Replication Manager ■ vCloud Availability vApp Replication Manager ■ vCloud Availability for Cloud-to-Cloud DR portal
Replicator Node	replicator	Deploys a dedicated vCloud Availability Replicator appliance.
Large Replicator Node	replicator_large	Deploys a dedicated vCloud Availability Replicator appliance suitable for large-scale environments.
Tunnel Node	tunnel	Deploys a vCloud Availability Tunnel appliance suitable for small-scale environments.

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

```
# echo $VMNAME

# ./ovftool/ovftool --name="${VMNAME}" --datastore="${VSPHERE_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-ip-address --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://$
{VCENTER_SERVER_USER}:VCENTER_SERVER_USER_PASSWORD@${VCENTER_SERVER_ADDRESS}${VSPHERE_LOCATOR}"
```

The system prints the IP address of the vCloud Availability for Cloud-to-Cloud DR appliance.

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 Manager, register the services within a single site, then pair your cloud sites.

The vCloud Availability for Cloud-to-Cloud DR 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 for Cloud-to-Cloud DR portal at `https://Appliance-IP-address/ui`. 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](#)
- [Configuring Cloud-to-Cloud Tunneling](#)
- [Pair Cloud Sites](#)

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

To configure vCloud Availability Replicator, vCloud Availability Replication Manager, and vCloud Availability vApp Replication Manager, use the service management interface of each component.

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/ui/admin`.

2 If you are prompted for Client Certificate, click **Cancel**.

The vCloud Availability Replicator service management interface login page opens.

3 Log in using the **root** password that you set during the OVA deployment.

The vCloud Availability Replicator **Getting Started** tab displays.

4 Change the **root** user password.

a Click **Change root password**.

The **vCloud Availability Appliance Password** window displays.

b Enter the **root** password that you set during the OVA deployment.

c Enter and confirm a new password.

Create a secured password with a minimum of eight characters and containing at least one of each of the following:

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

d Click **Apply**.

5 Click **Register in Lookup Service**.

The **Lookup Service Details** window displays.

6 Enter a valid lookup service address and click **Apply**.

Enter the lookup service address in the following format `https://Lookup-Service-IP-address:443/lookupservice/sdk`.

7 To complete the configuration, accept the SSL certificate of the lookup service.

You are redirected to the vCloud Availability Replicator **System Monitoring** 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/ui/admin`.
The vCloud Availability Replication Manager service management interface login page opens.
- 2 If you are prompted for Client Certificate, click **Cancel**.
- 3 Log in as **root**.
You are redirected to the **System Monitoring** tab.
- 4 If you deployed a **Combined** appliance, proceed to [Step 5](#). If you deployed a **Manager node with vCloud Director support**, change the **root** user password.
 - a Click **Change root password**.
The **vCloud Availability Appliance Password** window displays.
 - b Enter the **root** password that you set during the OVA deployment.
 - c Enter and confirm a new password.
Create a secured password with a minimum of eight characters and containing at least one of each of the following:
 - Lowercase: a b c
 - Uppercase: A B C
 - Numeric: 1 2 3
 - Special: & # %
 - d Click **Apply**.
- 5 Navigate to the **Configuration** tab and click **Edit** against the **Lookup service address** entry.
The **Lookup Service Details** window displays.
- 6 Enter a valid lookup service address and click **Apply**.
Enter the lookup service address in the following format `https://Lookup-Service-IP-address:443/lookupservice/sdk`.
- 7 To complete the configuration, accept the SSL certificate of the lookup service.

What to do next

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

Configure a vCloud Availability vApp Replication Manager

To configure a vCloud Availability vApp Replication Manager, enter a site name to 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.

Procedure

- 1 In a Web browser, go to `https://Appliance-IP-address/ui/admin`.
The vCloud Availability vApp Replication Manager service management interface login page opens.
- 2 If you are prompted for Client Certificate, click **Cancel**.
- 3 Log in as **root**.
You are redirected to the **Getting Started** tab.
- 4 Click **Run initial setup wizard**.
The **Initial Setup** wizard displays.
- 5 Enter a **Site Name** and optionally enter a **Site Description**, and click **Next**.

Important Note the site name that you enter, as it is used as an identifier and cannot be changed later.

- 6 Enter a valid lookup service address, single sign-on user name and password, and click **Next**.
Enter the lookup service address in the following format `https://Lookup-Service-IP-address:443/lookupservice/sdk`.
- 7 To complete configuration, accept the SSL certificate of the lookup service .
- 8 Set up vCloud Director.
 - a Select the **Configuration Type** and click **Next**.
If you select **Discover** the vCloud Director Service address automatically, proceed to [Step 9](#).
If you select **Enter details** for the vCloud Director Service manually, proceed to [Step 8b](#).

Option	Description
Discover the vCloud Director Service address automatically	By default, this option is selected. Use the option if the following configurations are present in your environment: <ul style="list-style-type: none"> ■ vCloud Director is federated with a previously specified lookup service. ■ There is only one registered vCloud Director in the lookup service. ■ The single sign-on user belongs to the System administrator group in vCloud Director.
Enter details for the vCloud Director Service manually	Select this option, if your vCloud Director instance is not federated with a previously specified lookup service or if multiple vCloud Director instances are registered to the lookup service.

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

- c Enter a vCloud Director **System administrator** user name and password, and click **Next**.
For example *administrator@system*, where *system* is the name of the system organization of vCloud Director.
The vCloud Director certificate details display.
 - d To complete the vCloud Director configuration, accept the vCloud Director SSL certificate.
- 9** Enter a valid vCloud Availability for Cloud-to-Cloud DR license key and click **Next**.
- 10** Select or deselect the **Join the VMware Customer Experience Improvement Program** check box to either join or leave the program and click **Next**.
VMware's Customer Experience Improvement Program provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products.
You are redirected to the **Ready to complete** tab.
- 11** Review the vCloud Availability vApp Replication Manager configuration summary and click **Finish**.
You are logged out and redirected to the vCloud Availability for Cloud-to-Cloud DR portal login page.
- 12** (Optional) Verify that the vCloud Availability vApp Replication Manager service is successfully configured.
- a In a Web browser, go to `https://Appliance-IP-address/ui/admin`.
 - b Log in with as **root**.
 - c Go to the **System Monitoring** tab and verify that there are no errors or alerts.

What to do next

If your scale target requires more than one vCloud Availability Replicator, you can add vCloud Availability Replicator instances. For more information, see [Add a New vCloud Availability Replicator](#).

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/ui/admin`.
The vCloud Availability Replication Manager service management interface login page opens.

- 2 Log in as **root**.
- 3 In the **Replicators** tab, click **New**.

The **New Replicator** wizard displays.

- 4 Enter the vCloud Availability Replicator details and click **Add**.

Option	Description
Site	Select the site where the vCloud Availability Replicator is deployed.
Description	You can optionally add a description for the vCloud Availability Replicator that you are registering.
API URL	The vCloud Availability Replicator API endpoint address. Enter the address in the <code>https://Replicator-Appliance-Address:8043</code> .
Appliance Password	The root user password for the vCloud Availability Replicator appliance.
SSO User Name	A user assigned with administrative privileges for the local site single sign-on domain, for example <code>Administrator@VSPHERE.LOCAL</code> .
SSO Password	The password for the administrative user.

If you enter the vCloud Availability Replicator FQDN, for example `eu-2.replicator.com`, the vCloud Availability Replication Manager service management interface displays the vCloud Availability Replicator appliance IP address instead of the FQDN.

- 5 To complete the registration, accept vCloud Availability Replicator SSL certificate.

The new vCloud Availability Replicator is added to the vCloud Availability Replication Manager.

Configuring Cloud-to-Cloud Tunneling

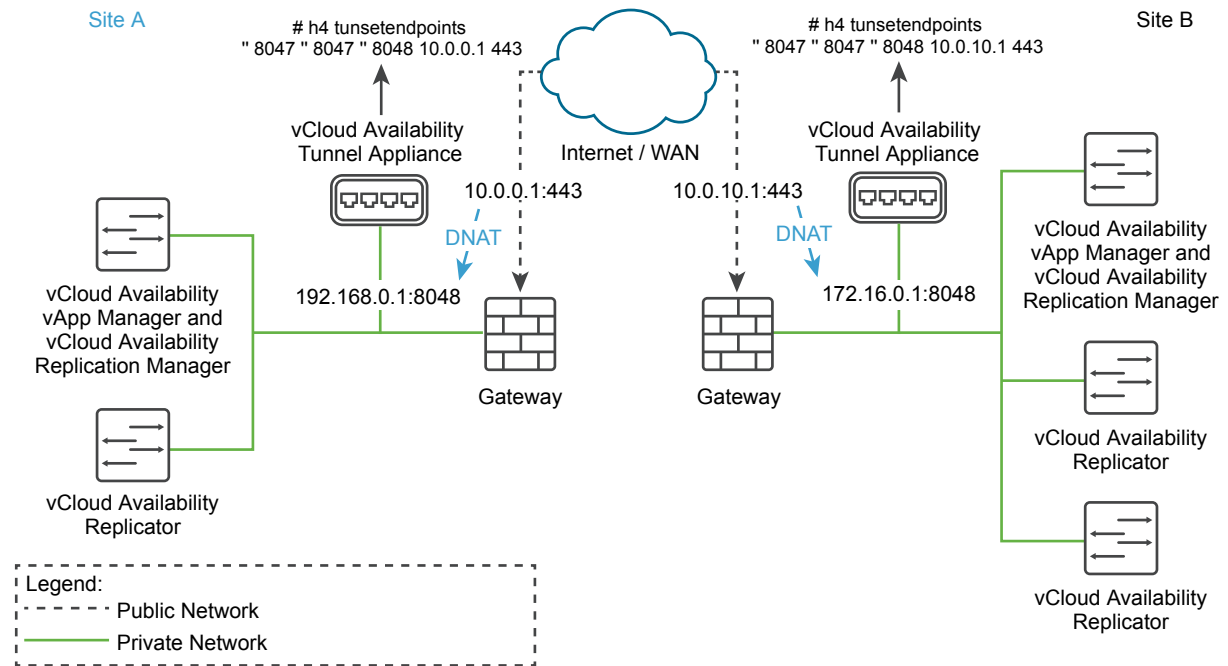
To establish a secure connection between two data centers, you can optionally configure Cloud-to-Cloud Tunneling.

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 allowing 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 diagram can help you understand a deployment where a Cloud-to-Cloud Tunneling is configured.



Configure Cloud-to-Cloud Tunneling by Using the vCloud Availability Tunnel Command-Line Interface

You can configure Cloud-to-Cloud Tunneling by creating an SSH connection to the vCloud Availability Tunnel appliance. Configure a vCloud Availability Tunnel appliance in all sites before pairing the cloud sites.

Prerequisites

- Verify that the following appliances are deployed:
 - vCloud Availability Replication Manager
 - vCloud Availability Replicator
 - vCloud Availability vApp Replication Manager
 - vCloud Availability Tunnel

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

- For all cloud 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 If you deployed a **Combined** appliance, proceed to [Step 3](#). If you deployed a **Tunnel Node**, you are prompted to change the **root** user password. Enter and confirm a new password.

Create a secured password with a minimum of eight characters and containing at least one of each of the following:

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

- 3 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` script 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
```

4 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
```

5 Save the /tmp/tunnel.pem file locally to your workstation.

6 Log in to the vCloud Availability vApp Replication Manager appliance console.

- a Open an SSH connection to the vCloud Availability vApp Replication Manager appliance.
- b Log in as **root**.

7 Upload the tunnel.pem file to the /tmp folder of the vCloud Availability vApp Replication Manager appliance.

8 Register the vCloud Availability Tunnel appliance to the vCloud Availability vApp Replication Manager appliance.

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

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

9 Reboot the vCloud Availability vApp Replication 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.

10 Reboot the vCloud Availability Replicator service.

- a In a Web browser, go to `https://Appliance-IP-address:8043/ui/admin`.
- b Log in as **root**.
- c In the **System Monitoring** tab, click **Restart Service**.

What to do next

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

Configure Cloud-to-Cloud Tunneling by Using the vCloud Availability for Cloud-to-Cloud DR Portal

You can configure Cloud-to-Cloud Tunneling by using the vCloud Availability for Cloud-to-Cloud DR portal. Configure a vCloud Availability Tunnel appliance in all your cloud sites before pairing the cloud sites.

Prerequisites

- For all cloud sites, verify that you have deployed the following appliances:
 - vCloud Availability Replication Manager
 - vCloud Availability Replicator
 - vCloud Availability vApp Replication Manager
 - vCloud Availability Tunnel

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

- For all cloud sites, verify that you have locally registered the vCloud Availability for Cloud-to-Cloud DR portal 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 for Cloud-to-Cloud DR portal.
 - a In a Web browser, go to `https://Appliance-IP-address/ui/admin`.
 - b Log in as **root**.
- 2 If you deployed a **Combined** appliance, proceed to [Step 3](#). If you deployed a **Tunnel Node**, change the **root** user password.
 - a Click **Change root password**.

The **vCloud Availability Appliance Password** widow displays.
 - b Enter the **root** password that you set during the OVA deployment.

- c Enter and confirm a new password.

Create a secured password with a minimum of eight characters and containing at least one of each of the following:

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

- d Click **Apply**.

- 3 Navigate to the **Configuration** tab and click **Edit** against the **Tunnel Address** entry.

The **Tunneling Settings** window displays.

- 4 Edit the Cloud-to-Cloud Tunneling settings and click **Apply**.

Option	Description
Enable tunneling for vCloud Availability services communication	To enable Cloud-to-Cloud Tunneling, select the option.
Tunnel address	The local vCloud Availability Tunnel appliance management endpoint. This address is used by the local vCloud Availability vApp Replication Manager for the automatic configuration of Cloud-to-Cloud Tunneling in the local vCloud Availability Tunnel appliance. By default, this address is the local appliance address and port <i>8047</i> , for example <code>https://Tunnel-IP-Address:8047</code> .
Appliance user	The vCloud Availability Tunnel appliance root user.
Password	The password for the vCloud Availability Tunnel appliance root user.

The vCloud Availability Tunnel appliance certificate details display.

- 5 To complete the configuration, accept the vCloud Availability Tunnel appliance SSL certificate.

- 6 In the **System Monitoring** tab, click **Restart Service** and confirm the operation.

You are logged out and are redirected to the vCloud Availability for Cloud-to-Cloud DR portal login page for tenants. Before you can proceed, wait for the services to restart.

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.

- 7 Reboot the vCloud Availability Replicator service.

- a In a Web browser, go to `https://Appliance-IP-address:8043/ui/admin`.
- b Log in as **root**.
- c In the **System Monitoring** tab, click **Restart Service**.

- 8 Verify if the local vCloud Availability Tunnel appliance is successfully configured.
 - a In a Web browser, go to `https://Appliance-IP-address/ui/admin`.
 - b Log in as **root**.
 - c In the **Cloud Sites** tab, verify that the vCloud Availability Tunnel appliance in the local site displays a green status.

What to do next

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

Pair Cloud Sites

By pairing your cloud sites, you establish a trust between vCloud Availability vApp Replication Manager instances in two different sites.

You can initiate pairing from either of the sites between which you establish a trust.

Prerequisites

Verify that you configured the following services in both sites between which you establish a trust:

- vCloud Availability vApp Replication Manager
- vCloud Availability Replication Manager
- vCloud Availability Replicator

Procedure

- 1 In a Web browser, go to `https://Appliance-IP-address/ui/admin`.
- 2 Log in as **root**.
- 3 In the **Cloud Sites** tab, click **New Cloud Site**.
- 4 Pair cloud sites.
 - a In the **New Cloud Site** pane, enter the name of the remote site.
 - b Enter the **Endpoint URL** of the remote site.
 - If you are not using Cloud-to-Cloud Tunneling, enter the address of the vCloud Availability vApp Replication Manager appliance in the remote site with port 8046. For example, `https://vApp-Replication-Manager-Appliance-IP-address:8046`.
 - If you are using Cloud-to-Cloud Tunneling, enter the public IP address of the vCloud Availability Tunnel appliance in the remote site with port 8048. For example, `https://Tunnel-Appliance-Public-IP-address:8048`.

- c To pair the local with the remote site, enable **Remote appliance credentials** and enter the **root** user password of the vCloud Availability vApp Replication Manager appliance.

To pair the sites with **Remote appliance credentials** disabled, you must repeat the procedure on your remote site.

- d Click **Pair**.

- e To complete the pairing, accept the SSL certificate of the remote vCloud Availability vApp Replication Manager appliance.

- 5 To verify that the trust between the two sites is successfully established, navigate to **Cloud Sites** and confirm that the new site is listed and there are no errors or warnings.

What to do next

Before you can configure replications, you must create a custom replication policy and assign it to the source and destination vCloud Director organizations, or edit the default replication policy for both organizations. The replication policy that is assigned to the source and destination organizations must allow replications. For more information, see *Working with Replication Policies* chapter in the *vCloud Availability for Cloud-to-Cloud DR User's Guide*.

Configuring the Customer Experience Improvement Program



When you choose to participate in the Customer Experience Improvement Program (CEIP), VMware receives anonymous information to improve the quality, reliability, and functionality of VMware products and services.

This chapter includes the following topics:

- [Categories of Information That VMware Receives](#)
- [Join or Leave the Customer Experience Improvement Program](#)

Categories of Information That VMware Receives

This product participates in the VMware Customer Experience Improvement Program (CEIP).

Details regarding the data collected by CEIP and the purposes for which it is used by VMware are available at the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>.

To join or leave the CEIP for this product, see [Join or Leave the Customer Experience Improvement Program](#).

Join or Leave the Customer Experience Improvement Program

You can choose to join the Customer Experience Improvement Program (CEIP), or leave the CEIP at any time.

Prerequisites

Verify that your user profile is assigned **System Administrator** privileges.

Procedure

- 1 Log in to the vCloud Availability for Cloud-to-Cloud DR portal as a **System administrator**. For more information, see [Accessing the vCloud Availability for Cloud-to-Cloud DR Portal as a Service Provider](#).
- 2 Navigate to **Configuration > System Settings > Participate in CEIP** and click **Edit**.
- 3 Select or deselect the **Join the VMware Customer Experience Improvement Program** checkbox to either join or leave the program and click **Apply**.

Upgrading vCloud Availability for Cloud-to-Cloud DR



You upgrade vCloud Availability for Cloud-to-Cloud DR components by using the service management interface of each of its components.

To upgrade to vCloud Availability for Cloud-to-Cloud DR 1.5, you can configure vCloud Availability for Cloud-to-Cloud DR components to download the upgrade packages from the following three sources.

- Download from the default VMware repository.
- Download from an ISO image file that is mounted to the CD-ROM drive of the component appliance.
- Download from a local repository, on which you have uploaded the upgrade package.

The following table describes the three options.

Option	Description
Default VMware Repository	Use the default VMware repository when your environment allows external Internet access. This option is configured by default.
Use CDROM Updates	Use the CD-ROM drive of a vCloud Availability for Cloud-to-Cloud DR appliance when your environment does not allow external Internet access.
Use Specified Repository	Use a specified local repository as a content mirror when your environment does not allow external Internet access and vCloud Availability for Cloud-to-Cloud DR appliances are deployed to multiple datastores.

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 Components by Using the Default VMware Repository](#)
- [Upgrade vCloud Availability for Cloud-to-Cloud DR by Using an ISO Image](#)
- [Upgrade vCloud Availability for Cloud-to-Cloud DR Components by Using a Specified Repository](#)
- [Install the vCloud Availability for Cloud-to-Cloud DR Plug-In for vCloud Director](#)
- [Start Working with vCloud Availability for Cloud-to-Cloud DR 1.5](#)

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.

Upgrade vCloud Availability for Cloud-to-Cloud DR components in the local site and then upgrade all components in the remote site. During the upgrade, you might observe replication interruptions and Recovery Point Objective (RPO) violations.

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

- 1 Upgrade all vCloud Availability vApp Replication Manager instances.
- 2 Upgrade all vCloud Availability Replication Manager instances.
- 3 Upgrade all vCloud Availability Replicator instances.
- 4 If you use Cloud-to-Cloud Tunneling, upgrade all vCloud Availability Tunnel instances.

Upgrade vCloud Availability for Cloud-to-Cloud DR Components by Using the Default VMware Repository

You can configure vCloud Availability for Cloud-to-Cloud DR components to download the upgrade package from the default VMware repository.

Procedure

- 1 Log in to the service management interface for the vCloud Availability for Cloud-to-Cloud DR component as **root**.

You access service management interfaces for vCloud Availability for Cloud-to-Cloud DR components in a Web browser. The following table lists the services management interface addresses of vCloud Availability for Cloud-to-Cloud DR components.

Table 8-1. Services Management Interface Addresses

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

- 2 Install updates.
 - a In the **Update** tab, click **Check Updates** and wait for the check to complete.
 - b Click **Install Updates** and wait for the update to install.

Installing the updates logs you out from your Web session.

- 3 After the upgrade completes successfully, log in to the service management interface for the vCloud Availability for Cloud-to-Cloud DR component as **root**.
- 4 In the **System Monitoring** tab, click **Reboot VM**.

What to do next

After you upgrade all vCloud Availability for Cloud-to-Cloud DR components in all sites, you finalize the upgrade by carrying out the post-upgrade configuration. For more information, see [Start Working with vCloud Availability for Cloud-to-Cloud DR 1.5](#).

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

You can configure vCloud Availability for Cloud-to-Cloud DR components to download the upgrade package from an ISO image file that is mounted to the CD-ROM drive of the component appliance.

Procedure

- 1 Download the `vCloud-Availability-C2C-1.5.XXX-build_number.iso` image from the vCloud Availability for Cloud-to-Cloud DR official VMware download site.
- 2 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.
- 3 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 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.
- 4 Log in to the service management interface for the vCloud Availability for Cloud-to-Cloud DR component as **root**.

You access service management interfaces for vCloud Availability for Cloud-to-Cloud DR components in a Web browser. The following table lists the services management interface addresses of vCloud Availability for Cloud-to-Cloud DR components.

Table 8-2. Services Management Interface Addresses

vCloud Availability for Cloud-to-Cloud DR Component	Management Interface Address and Port
vCloud Availability vApp Replication Manager	<code>https://Appliance-IP-Address:8046/ui/admin</code>
vCloud Availability Replication Manager	<code>https://Appliance-IP-Address:8044/ui/admin</code>

Table 8-2. Services Management Interface Addresses (Continued)

vCloud Availability for Cloud-to-Cloud DR Component	Management Interface Address and Port
vCloud Availability Replicator	https://Appliance-IP-Address:8043/ui/admin
vCloud Availability Tunnel	https://Appliance-IP-Address:8047/ui/admin

- 5 Install updates.
 - a Navigate to **Update > Settings**.
 - b Select the **Use CDROM Updates** option.
 - c In the **Update** tab, click **Check Updates** and wait for the check to complete.
 - d Click **Install Updates** and wait for the update to install.
Installing the updates logs you out from your Web session.
- 6 After the upgrade completes successfully, log in to the service management interface for the vCloud Availability for Cloud-to-Cloud DR component as **root**.
- 7 In the **System Monitoring** 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.
 - 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.

What to do next

After you upgrade all vCloud Availability for Cloud-to-Cloud DR components in all sites, you finalize the upgrade by carrying out the post-upgrade configuration. For more information, see [Start Working with vCloud Availability for Cloud-to-Cloud DR 1.5](#).

Upgrade vCloud Availability for Cloud-to-Cloud DR Components by Using a Specified Repository

You can configure vCloud Availability for Cloud-to-Cloud DR components to use a local repository, on which you have uploaded the upgrade package.

Procedure

- 1 Prepare the local repository for upgrades.
 - a Install and configure a local Web server.
 - b Download the `vCloud-Availability-C2C-1.5.XXX-build_number.iso` file from the official VMware download site.
 - c Mount the ISO image and copy the update directory to the local Web server.

The update directory should contain `manifest` and `package-pool` directories.

- 2 Log in to the service management interface for the vCloud Availability for Cloud-to-Cloud DR component as **root**.

You access service management interfaces for vCloud Availability for Cloud-to-Cloud DR components in a Web browser. The following table lists the services management interface addresses of vCloud Availability for Cloud-to-Cloud DR components.

Table 8-3. Services Management Interface Addresses

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

- 3 Install updates.
 - a Navigate to **Update > Settings** and select the **Use Specified Repository** option.
 - b Enter the URL address of the local repository by pointing to the update directory of the local Web server.
For example, `http://local-web-server-address/update`.
 - c If the local repository requires authentication, enter user name and password.
 - d Click **Save Settings**.
 - e In the **Update** tab, click **Check Updates** and wait for the check to complete.
 - f Click **Install Updates** and wait for the update to install.

Installing the updates logs you out from your Web session.

- 4 After the upgrade completes successfully, log in to the service management interface for the vCloud Availability for Cloud-to-Cloud DR component as **root**.
- 5 In the **System Monitoring** tab, click **Reboot VM**.

What to do next

After you upgrade all vCloud Availability for Cloud-to-Cloud DR components in all sites, you finalize the upgrade by carrying out the post-upgrade configuration. For more information, see [Start Working with vCloud Availability for Cloud-to-Cloud DR 1.5](#).

Install the vCloud Availability for Cloud-to-Cloud DR Plug-In for vCloud Director

To access the vCloud Availability for Cloud-to-Cloud DR portal from the **vCloud Director Service Provider Admin Portal** and the **vCloud Director Tenant Portal**, you must install the vCloud Availability for Cloud-to-Cloud DR plug-in for vCloud Director.

Procedure

- 1 Log in to the vCloud Availability for Cloud-to-Cloud DR portal as a service provider.
 - a In a Web browser, go to `https://vApp-Replication-Manager-IP-address/ui/admin`.
 - b Log in as **root**.
- 2 Install the vCloud Availability for Cloud-to-Cloud DR plug-in for vCloud Director.
 - a Navigate to the **Configuration** tab and click **Edit** against the **vCloud Director address** entry.
 - b Select the configuration type and click **Apply**.

If you select **Discover** the vCloud Director Service address automatically, proceed to [Step 3](#).

If you select **Enter details** for the vCloud Director Service manually, proceed to [Step 2c](#).

Option	Description
Discover the vCloud Director Service address automatically	By default, this option is selected. Use the option if the following configurations are present in your environment: <ul style="list-style-type: none"> ■ vCloud Director is federated with a previously specified lookup service. ■ There is only one registered vCloud Director in the lookup service. ■ The single sign-on user belongs to the System administrator group in vCloud Director.
Enter details for the vCloud Director Service manually	Select this option, if your vCloud Director instance is not federated with a previously specified lookup service or if multiple vCloud Director instances are registered to the lookup service.

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

- d Enter a vCloud Director **System administrator** user name and password, and click **Next**.
For example *administrator@system*, where *system* is the name of the system organization of vCloud Director.
The vCloud Director certificate details display.
- e To finish the vCloud Director configuration, accept the vCloud Director SSL certificate.

- 3 In the **System Monitoring** tab, click **Restart Service** and confirm the operation.

After the operation finishes, you are logged out of the vCloud Availability for Cloud-to-Cloud DR portal.

You successfully installed the vCloud Availability for Cloud-to-Cloud DR plug-in for vCloud Director and can access the vCloud Availability for Cloud-to-Cloud DR portal directly from the vCloud Director user interface.

Start Working with vCloud Availability for Cloud-to-Cloud DR 1.5

After you upgrade all vCloud Availability for Cloud-to-Cloud DR components in the local and the remote sites, to start working with vCloud Availability for Cloud-to-Cloud DR 1.5, verify that the trust between cloud sites is preserved, enter a valid license key, and configure replication policies in the local and the remote sites.

Procedure

- 1 Log in to the vCloud Availability for Cloud-to-Cloud DR portal.
 - a In a Web browser, go to `https://Appliance-IP-address/ui/admin`.
 - b Log in as **root**.
- 2 If the **Cloud Sites** tab reports no errors, proceed to [Step 3](#). If the **Cloud Sites** tab reports errors, you must reestablish the trust between the cloud sites. See [Reestablish Cloud Sites Trust](#).
- 3 Enter a valid vCloud Availability for Cloud-to-Cloud DR license key.
 - a In the **Configuration** tab, click **Edit** against the **License key** entry.
 - b Enter your license key and click **Apply**.
 - c Verify that there are no errors in against the **License key** entry.
- 4 Create custom replication policies or enable configuring replication in the default policy.

To configure new replications, the policies that are assigned to the source and the destination vCloud Director organizations must allow incoming and outgoing replications.

You create and edit replication policies by using the vCloud Availability for Cloud-to-Cloud DR portal.

To manage replication policies, you must log in to the vCloud Availability for Cloud-to-Cloud DR portal as a service provider. For more information about accessing the vCloud Availability for Cloud-to-Cloud DR portal and working with replication policies, see the *vCloud Availability for Cloud-to-Cloud DR User's Guide*.

You successfully upgraded vCloud Availability for Cloud-to-Cloud DR and can start configuring replications. For more information, see the *vCloud Availability for Cloud-to-Cloud DR User's Guide*.

Managing vCloud Availability for Cloud-to- Cloud DR

9

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

This chapter includes the following topics:

- [Add a New vCloud Availability Replicator](#)
- [Reestablish Cloud Sites Trust](#)
- [Certificate Management in vCloud Availability for Cloud-to-Cloud DR](#)
- [Collect vCloud Availability for Cloud-to-Cloud DR Usage Information](#)
- [Collect vCloud Availability for Cloud-to-Cloud DR Storage Consumption Information](#)
- [Troubleshooting vCloud Availability for Cloud-to-Cloud DR](#)

Add a New vCloud Availability Replicator

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

Prerequisites

- Make sure that vCloud Availability Replicator, vCloud Availability Replication Manager, and vCloud Availability vApp Replication Manager are configured in your environment.
- Deploy a new vCloud Availability Replicator appliance. For more information, see [Chapter 4 Deploy vCloud Availability for Cloud-to-Cloud DR Services Using the vSphere Web Client](#) and [Deploy vCloud Availability for Cloud-to-Cloud DR Services Using the OVF Tool](#).
- Configure the new vCloud Availability Replicator appliance. For more information, see [Configure a vCloud Availability Replicator](#).
- Register the new vCloud Availability Replicator appliance to the local 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 Add a vCloud Availability Replicator.
 - a In a Web browser, go to `https://Appliance-IP-address:8044/ui/admin`.
The vCloud Availability Replication Manager service management interface login page displays.
 - b Log in as **root**.
 - c In the **Replicators** tab, click **New**.
The **New Replicator** wizard displays.
 - d Select the site to which you add the new vCloud Availability Replicator instance.
 - e (Optional) Add a description for the vCloud Availability Replicator.
 - f In the **API URL** text box, enter the vCloud Availability Replicator appliance address and port 8043.
For example, `https://Appliance-IP-address:8043`.
 - g Enter the appliance **root** password that you set during the initial vCloud Availability Replicator configuration.
 - h Enter the single sign-on domain administrator user name and password.
For example, `administrator@vsphere.local`.
 - i Click **Add**.
 - j To complete the addition, accept the vCloud Availability Replicator SSL certificate.
- 2 If you use Cloud-to-Cloud Tunneling, register the vCloud Availability Tunnel appliance to the new vCloud Availability Replicator.
 - a Log in to the vCloud Availability Replicator console as **root**.

```
$ h4 rtrloginroot Replicator-root-password
```
 - b Register the vCloud Availability Tunnel appliance.

```
$ h4 rtrregtunnel Local-Tunnel-Appliance-IP-Address Tunnel-Appliance-Port-Number
```
 - c Reboot the vCloud Availability Replicator.

```
$ systemctl restart replicator
```

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

What to do next

To use the new vCloud Availability Replicator instance, reestablish the trust between cloud sites. See [Reestablish Cloud Sites Trust](#).

Reestablish Cloud Sites Trust

After you add a vCloud Availability Replicator, replace the vCloud Availability vApp Replication Manager certificate, or upgrade vCloud Availability for Cloud-to-Cloud DR, you must reestablish the trust between the cloud sites.

You can initiate the trust reestablishment from either of the sites between which you establish a trust.

Procedure

- 1 In a Web browser, go to `https://Appliance-IP-address/ui/admin`.
- 2 Log in as **root**.
- 3 In the **Cloud Sites** tab, click the drop-down menu for the peer site and click **Repair**.
- 4 In the **Sites administration** window, enter the **root** user password of the remote vCloud Availability vApp Replication Manager appliance and click **Update**.
- 5 To complete the trust reestablishment, accept the SSL certificate of the remote vCloud Availability vApp Replication Manager appliance.

You reestablished the cloud sites trust and can configure new incoming and outgoing replications between the sites.

Certificate Management in vCloud Availability for Cloud-to-Cloud DR

When you renew or replace the SSL certificate of a vCloud Availability for Cloud-to-Cloud DR service, you must reconfigure the remaining services of vCloud Availability for Cloud-to-Cloud DR to work with the new certificate.

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 to use the new certificate. For more information, see <https://kb.vmware.com/s/article/2118939>.
- Make sure that all components in your environment that depend on the vCenter Server registration in the Lookup Service are configured to trust 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 all vCloud Availability Replicator instances.

- a In a Web Browser, navigate to the vCloud Availability Replicator service management interface at <https://Appliance-IP-Address:8043/ui/admin>.

- b Log in as **root**.

- c Navigate to the **Configuration** tab and click **Edit** against the **Lookup service address** entry.

- d Enter the Lookup Service address and click **Apply**.

The details of the new certificate appear.

- e To complete the vCloud Availability Replicator configuration, 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 service management interface at <https://Appliance-IP-Address:8044/ui/admin>.

- b Log in as **root**.

- c Navigate to the **Configuration** tab and click **Edit** against the **Lookup service address** entry.

- d Enter the Lookup Service address and click **Apply**.

The details of the new certificate appear.

- e To complete the vCloud Availability Replication Manager configuration, accept the new Lookup Service certificate.

- 3 Configure the vCloud Availability vApp Replication Manager to work with the new PSC certificate.

- a In a Web Browser, navigate to the vCloud Availability vApp Replication Manager Configuration Portal at <https://Appliance-IP-Address/ui/admin>.

- b Log in as **root**.

- c Navigate to the **Configuration** tab and click **Edit** against the **Lookup service address** entry.

- d Enter the Lookup Service address and click **OK**.

The details of the new certificate appear.

- e To complete the vCloud Availability vApp Replication Manager configuration, 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 all vCloud Availability Replicator instances.

- a In the vCloud Availability Replicator service management interface, go to **System Monitoring**.
- b Click **Restart Services**.
- c Confirm the restart by clicking **Restart** in the pop-up window.

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

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

The procedure is known to work with 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 Manager appliance console as an **root**.
- 2 Copy the *custom.p12* archive that contains the externally signed certificate to the /tmp folder of the vCloud Availability vApp Replication Manager appliance.
- 3 Create a backup copy of the certificate that is used by vCloud Availability vApp Replication 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 Manager appliance.

5 Import the new keystore to the vCloud Availability vApp Replication 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 Manager appliance.

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

7 Restart the vCloud Availability vApp Replication Manager services:

```
$ systemctl restart cloud
```

The vCloud Availability vApp Replication 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
```

What to do next

To configure new replications with vCloud Availability for Cloud-to-Cloud DR, reestablish the trust between cloud sites. See [Reestablish Cloud Sites Trust](#).

Renew the SSL Certificate of the vCloud Availability Replicator Service

When the SSL certificate of the vCloud Availability Replicator service expires, you use the service management interface of the service to regenerate the certificate.

Regenerating the SSL certificate of the vCloud Availability Replicator service breaks the registration of the vCloud Availability Replicator service to the vCloud Availability Replication Manager instance in the local and remote sites.

After you renew the SSL Certificate of the vCloud Availability Replicator service, to repair the registration to the vCloud Availability Replication Manager instance in the remote site, reestablish the trust between the cloud sites.

Procedure

- 1 Log in to the service management interface of the vCloud Availability Replicator service.
 - a In a Web browser, go to `https://Appliance-IP-address:8043/ui/admin`.
 - b Log in as **root**.
- 2 Regenerate the SSL certificate of the vCloud Availability Replicator service.
 - a Navigate to the **Configuration** tab and click **Regenerate** against the **Certificate** entry.
 - b Confirm the operation by clicking **Apply**.

Regenerating the SSL certificate of the vCloud Availability Replicator service restarts all vCloud Availability Replicator services that run on the same appliance.

After the operation finishes, you are logged out of the service management interface of the vCloud Availability Replicator service.

- 3 Repair the registration to the vCloud Availability Replication Manager service in the local site.
 - a In a Web browser, go to the service management interface of the vCloud Availability Replication Manager service at `https://Appliance-IP-address:8044/ui/admin`.
 - b Log in as **root**.

The **System Monitoring** tab displays that the vCloud Availability Replicator instance that uses a new SSL certificate is **Offline**.
 - c In the **Replicators** tab, select the vCloud Availability Replicator instance and click **Repair**.
 - d Enter details of the vCloud Availability Replicator service and click **Apply**.

Option	Description
Appliance Password	The root user password for the vCloud Availability Replicator appliance.
SSO User Name	A user assigned with administrative privileges for the local site single sign-on domain, for example <code>Administrator@VSPHERE.LOCAL</code> .
SSO Password	The password for the administrative user.

- e Verify that no errors are reported in the **System Monitoring** tab.

You successfully renewed the SSL certificate of the vCloud Availability Replicator service.

What to do next

To configure new replications, you must reestablish the trust between the cloud sites. See [Reestablish Cloud Sites Trust](#).

Renew the SSL Certificate of the vCloud Availability Replication Manager Service

When the SSL certificate of the vCloud Availability Replication Manager service expires, you use the service management interface of the vCloud Availability Replication Manager service to regenerate the certificate.

Regenerating the SSL certificate of the vCloud Availability Replication Manager service breaks the registration of the vCloud Availability Replicator instances in the local and remote sites to the vCloud Availability Replication Manager service in the local site.

After you renew the SSL Certificate of the vCloud Availability Replication Manager service, to repair the registration of vCloud Availability Replicator instances in the remote site, reestablish the trust between the cloud sites.

Procedure

- 1 Log in to the service management interface of the vCloud Availability Replication Manager service.
 - a In a Web browser, go to `https://Appliance-IP-address:8044/ui/admin`.
 - b Log in as **root**.
- 2 Regenerate the SSL certificate of the vCloud Availability Replication Manager service.
 - a Navigate to the **Configuration** tab and click **Regenerate** against the **Certificate** entry.
 - b Confirm the operation by clicking **Apply**.

Regenerating the SSL certificate of the vCloud Availability Replication Manager service restarts all vCloud Availability Replicator services that run on the same appliance. After the operation finishes, you are logged out of the service management interface of the vCloud Availability Replication Manager service.

- 3 Repair the registration of vCloud Availability Replicator instances to the vCloud Availability Replication Manager service in the local site.
 - a Log in to the service management interface of the vCloud Availability Replication Manager appliance again.

The **System Monitoring** tab displays that all vCloud Availability Replicator instances are **OffLine**.
 - b In the **Replicators** tab, select a vCloud Availability Replicator instance and click **Repair**.
 - c Enter details of the vCloud Availability Replicator instance and click **Apply**.

Option	Description
Appliance Password	The root user password for the vCloud Availability Replicator appliance.
SSO User Name	A user assigned with administrative privileges for the local site single sign-on domain, for example <code>Administrator@VSPHERE.LOCAL</code> .
SSO Password	The password for the administrative user.

- d Accept the SSL certificate of the vCloud Availability Replicator service.
- e Repeat [Step 3b](#) through [Step 4d](#) for all vCloud Availability Replicator instances that are registered to the vCloud Availability Replication Manager service in the local site.
- f After you repair the registrations for all vCloud Availability Replicator instances, verify that no connectivity errors are reported in the **System Monitoring** tab.

You successfully renewed the SSL certificate of the vCloud Availability Replication Manager service.

What to do next

To configure new replications, you must reestablish the trust between the cloud sites. See [Reestablish Cloud Sites Trust](#).

Renew the SSL Certificate of the vCloud Availability vApp Replication Manager Service

When the SSL certificate of the vCloud Availability vApp Replication Manager service expires, you use the vCloud Availability for Cloud-to-Cloud DR portal to regenerate the certificate.

Regenerating the SSL certificate of the vCloud Availability vApp Replication Manager service breaks the trust between the cloud sites. After you renew the SSL Certificate of the vCloud Availability vApp Replication Manager service, you must reestablish the trust between the cloud sites.

Procedure

- 1 Log in to the vCloud Availability for Cloud-to-Cloud DR portal.
 - a In a Web browser, go to `https://Appliance-IP-address/ui/admin`.
 - b Log in as **root**.
- 2 Regenerate the SSL certificate of the vCloud Availability vApp Replication Manager service.

Regenerating the SSL certificate of the vCloud Availability vApp Replication Manager service restarts all vCloud Availability Replicator services that run on the same appliance.

 - a Navigate to the **Configuration** tab and click **Regenerate** against the **Certificate** entry.
 - b Confirm the operation by clicking **Apply**.

After the operation finishes, you are logged out of the vCloud Availability for Cloud-to-Cloud DR portal.

If you do not use Cloud-to-Cloud Tunneling, you successfully regenerated the SSL certificate of the vCloud Availability vApp Replication Manager service and must reestablish the trust between the cloud sites.

If you use Cloud-to-Cloud Tunneling, proceed to [Step 3](#).

- 3 Log in to the vCloud Availability for Cloud-to-Cloud DR portal again.
 - a In a Web browser, go to `https://Appliance-IP-address/ui/admin`.
 - b Log in as **root**.
- 4 Authenticate to the vCloud Availability vApp Replication Manager appliance in the remote site.
 - a Navigate to the **Configuration** tab and click **Edit** against the **Tunnel address** entry.
 - b Enter the **root** password for the vCloud Availability vApp Replication Manager appliance in the remote site and click **Apply**.

You successfully regenerated the SSL certificate of the vCloud Availability vApp Replication Manager service.

What to do next

To configure new replications, you must reestablish the trust between the cloud sites. See [Reestablish Cloud Sites Trust](#).

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 Manager appliance console as **root**.

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

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

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

- 3 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 in the following format:

```
# vCloud Availability C2C DR Usage Report

generatedOn    2018-09-11 08:28:48.246639
productName    vSphere Replication Cloud (C4)
```

```

buildVersion 1.5.0.1126-b60fa40
localSite    site2
instanceId   86f3279d-4119-4c0a-9a30-7295cdbda4d1

Total incoming vApp replications          1
Newly started incoming vApp replications  0
Carried over incoming vApp replications  0
Total incoming VM replications            1
Newly started incoming VM replications    0
Carried over incoming VM replications     0

Incoming vApp replications by org
Org    Org Id  Number of Replications
s2Org  c6415681-9456-4051-88bd-5b3ebf75f610  1

Incoming VM replications by org
Org    Org Id  Number of Replications
s2Org  c6415681-9456-4051-88bd-5b3ebf75f610  1

Incoming vApp replications by vDC
vDC    vDC Id  Org    Number of Replications
vdc_s2Org  f5aed876-4d62-4c35-9d3d-9c3065a8bcfb  s2Org  1

Incoming VM replications by vDC
vDC    vDC Id  Org    Number of Replications
vdc_s2Org  f5aed876-4d62-4c35-9d3d-9c3065a8bcfb  s2Org  1

# End of report.

```

The `/tmp/report_details.tsv` file contains information about individual incoming replications in the following format:

```

# vCloud Availability C2C DR Detailed Usage Report

generatedOn 2018-09-11 08:28:48.246639
productName vSphere Replication Cloud (C4)
buildVersion 1.5.0.1126-b60fa40
localSite    site2
instanceId   86f3279d-4119-4c0a-9a30-7295cdbda4d1

Total incoming vApp replications          1
Newly started incoming vApp replications  0
Carried over incoming vApp replications  0
Total incoming VM replications            1
Newly started incoming VM replications    0
Carried over incoming VM replications     0

Incoming VM Replications
vApp Name      vApp Id VM Name VM Id  Replication ID Source Site    Source Org    Source vDC
Id Source vDC  Destination Site      Destination Org Id  Destination Org Destina
tion vDC Id    Destination vDC

```

```
r001      51b08709-c0c5-4313-8ca1-e032cd6cd988      r001      859a28f8-6415-4e95-a9c8-38ed1ba66cff
C4-3b85e45e-3687-4e05-ba81-8bb95b1088a4  site1  s10rg  37642bdd-4e25-461c-8a2f-9082072ee3e9  v
dc_s10rg      site2  c6415681-9456-4051-88bd-5b3ebf75f610      s20rg
f5aed876-4d62-4c35-9d3d-9c3065a8bcfb  vdc_s20rg
```

- 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
```

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

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

Collect vCloud Availability for Cloud-to-Cloud DR Storage Consumption Information

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

To aggregate a detailed monthly storage consumption report, create daily snapshots by using the `storage-report -s`. At the end of the reporting period, generate an aggregated storage consumption report by using the `storage-report`. The `storage-report` script reads all storage consumption snapshots that you created and generates an aggregated report of the average storage consumption.

Procedure

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

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

- Create a storage consumption snapshot.

```
$ storage-report -s
```

The `storage-report -s` script saves the storage consumption information at the time the script runs.

The system returns the storage consumption snapshot data in the following format:

```
# vCloud Availability C2C DR - snapshot Storage Consumption Report

generatedOn      2018-09-11 08:28:34.474680
productName      vSphere Replication Cloud (C4)
buildVersion     1.5.0.1126-b60fa40
localSite        site2
instanceId       86f3279d-4119-4c0a-9a30-7295cdbda4d1

Storage consumption by org
```

```

Org      Org Id  Storage consumed      Number of PITs
s2Org   c6415681-9456-4051-88bd-5b3ebf75f610  10486784      0

Storage consumption by vDC
vDC      vDC Id  Org      Storage consumed      Number of PITs
vdc_s2Org      f5aed876-4d62-4c35-9d3d-9c3065a8bcfb  s2Org  10486784      0

# End of report.

```

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

```
$ storage-report --help
```

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

```
$ storage-report --output /tmp/storage_report.tsv
```

Running the `storage-report` script deletes all previously created snapshots. Run the `storage-report` script in the end of a reporting period to aggregate storage snapshots for the ending reporting period and prepare the system for the next reporting period.

The aggregated storage consumption report uses the following format:

```

# vCloud Availability C2C DR - aggregated Storage Consumption Report

generatedOn    2018-09-11 08:28:58.288823
productName    vSphere Replication Cloud (C4)
buildVersion   1.5.0.1126-b60fa40
localSite      site2
instanceId     86f3279d-4119-4c0a-9a30-7295cdbda4d1

Storage consumption by org (avg)
Org      Org Id  Storage consumed      Number of PITs
s2Org   c6415681-9456-4051-88bd-5b3ebf75f610  10486784      0

Storage consumption by vDC (avg)
vDC      vDC Id  Org      Storage consumed      Number of PITs
vdc_s2Org      f5aed876-4d62-4c35-9d3d-9c3065a8bcfb  s2Org  10486784      0

# End of report.

```

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

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

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

```
$ rm /tmp/storage_report.tsv
```

Troubleshooting

vCloud Availability for Cloud-to-Cloud DR

Known troubleshooting information can help you diagnose and correct problems in your disaster recovery environment.

Set or Update a Network Time Protocol Configuration

You set or update the Network Time Protocol (NTP) configuration by using the appliance console.

Problem

If you do not set an NTP server during the deployment of vCloud Availability for Cloud-to-Cloud DR appliances, or if you use different NTP servers for components in your disaster recovery environment, you might encounter connection or authentication problems.

Cause

To avoid connection or authentication problems, the following components of your disaster recovery environment must use the same time synchronization configuration:

- All vCenter Server instances in the source and destination sites
- All ESXi hosts in the source and destination sites
- Platform Services Controller instances in the source and destination sites
- All vCloud Availability for Cloud-to-Cloud DR appliances in the source and destination sites

Solution

- 1 Log in to the affected vCloud Availability for Cloud-to-Cloud DR appliance.
 - a Open an SSH connection to the affected appliance.
 - b Log in as **root**.
- 2 Using a text editor, for example `vi`, open the `/etc/systemd/timesyncd.conf` file.
- 3 To set or update the NTP server of the appliance, modify the following entry.
`NTP=NTP-Server-Address`
- 4 Save the changes and exit the text editor.
- 5 Restart the time synchronization service by running the following command.

```
$ systemctl restart systemd-timesyncd
```

What to do next

Set or update the same NTP configuration in all vCloud Availability for Cloud-to-Cloud DR appliances.

Cannot Access vCloud Availability for Cloud-to-Cloud DR Portal Through vCloud Director

You cannot access the vCloud Availability for Cloud-to-Cloud DR portal through the **vCloud Director Service Provider Admin Portal** and the **vCloud Director Tenant Portal**.

Problem

The Availability option is not available in the **vCloud Director Service Provider Admin Portal** and the **vCloud Director Tenant Portal** or the option is available, but clicking it does not open the vCloud Availability for Cloud-to-Cloud DR portal. In the vCloud Availability for Cloud-to-Cloud DR logs, you see that an exception occurred and the following error is present: Unable to register vCAV plugin in vCD.

Cause

Connectivity problems during the initial configuration of vCloud Availability for Cloud-to-Cloud DR might prevent the vCloud Availability for Cloud-to-Cloud DR plug-in from registering to vCloud Director.

Solution

- 1 Log in to the vCloud Availability for Cloud-to-Cloud DR portal as a service provider.
 - a In a Web browser, go to `https://vApp-Replication-Manager-IP-address/ui/admin`.
 - b Log in as **root**.
- 2 Register the vCloud Availability for Cloud-to-Cloud DR plug-in to vCloud Director.
 - a Navigate to the **Configuration** tab and click **Edit** against the **vCloud Director address** entry.
 - b Select the configuration type and click **Apply**.

If you select **Discover** the vCloud Director Service address automatically, proceed to [Step 3](#).

If you select **Enter details** for the vCloud Director Service manually, proceed to [Step 2c](#).

Option	Description
Discover the vCloud Director Service address automatically	By default, this option is selected. Use the option if the following configurations are present in your environment: <ul style="list-style-type: none"> ■ vCloud Director is federated with a previously specified lookup service. ■ There is only one registered vCloud Director in the lookup service. ■ The single sign-on user belongs to the System administrator group in vCloud Director.
Enter details for the vCloud Director Service manually	Select this option, if your vCloud Director instance is not federated with a previously specified lookup service or if multiple vCloud Director instances are registered to the lookup service.

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

- d Enter a vCloud Director **System administrator** user name and password, and click **Next**.

For example *administrator@system*, where *system* is the name of the system organization of vCloud Director.

The vCloud Director certificate details display.

- e To complete the vCloud Director configuration, accept the vCloud Director SSL certificate.

- 3 In the **System Monitoring** tab, click **Restart Service** and confirm the operation.

After the operation finishes, you are logged out of the vCloud Availability for Cloud-to-Cloud DR portal

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** user name and password, 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 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/ui/admin`.
The vCloud Availability Replicator service management interface login page opens.
- 2 Log in as **root**.
- 3 Go to **Support**.

- 4 Click **Generate New** and confirm the operation by clicking **Generate**.

A pop-up window indicating the process progress appears.

- 5 After the bundle is generated, to save the support bundle file locally, click on the bundle and confirm by clicking **Download**.

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/ui/admin`.

The vCloud Availability Replication Manager service management interface login page opens.

- 2 Log in as **root**.
- 3 Go to **Support**.
- 4 Click **Generate New** and confirm the operation by clicking **Generate**.

A pop-up window indicating the process progress appears.

- 5 After the bundle is generated, to save the support bundle file locally, click on the bundle and confirm by clicking **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 vApp Replication Manager

To collect the support bundle for vCloud Availability vApp Replication Manager by using the appliance graphic user interface, perform the following steps:

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

The vCloud Availability vApp Replication Manager service management interface login page opens.

- 2 Log in as **root**.
- 3 Go to **Support**.
- 4 Click **Generate New** and confirm the operation by clicking **Generate**.

A pop-up window indicating the process progress appears.

- 5 After the bundle is generated, to save the support bundle file locally, click on the bundle and confirm by clicking **Download**.

Collecting vCloud Availability for Cloud-to-Cloud DR Logs by Using Command Line Interface

To collect the support bundle for vCloud Availability vApp Replication Manager by using the appliance command-line interface, perform the following steps:

- 1 Create an SSH connection to the vCloud Availability vApp Replication Manager and log in as **root**.

- 2 Create a folder to store the support bundles.

```
# mkdir bundles
```

- 3 Run the `/opt/vmware/h4/bin/support-bundle.py` script.

You must provide the deployment type of your appliance and the output folder as arguments to the script. If you deployed a combined type appliance, the script collects all logs from the virtual machine. If you used other deployment types, you must create an SSH connection to each vCloud Availability for Cloud-to-Cloud DR appliance and run the script providing the respective deployment type and output folder as arguments. Following is an example of the command used to collect logs from a combined appliance:

```
# /opt/vmware/h4/bin/support-bundle.py combined ./bundles
```

Upon a successful creation of the support bundle file, you receive the following message: The support bundle was successfully generated at `/root/bundles/bundle-YYYY-MM-DD_HH-mm-SS-Time-Zone/combined-bundle-YYYY-MM-DD_HH-mm-SS-Time-Zone.tar.bz2`.

- 4 Copy the logs archive to your machine.