

Administering vCloud Availability

VMware vCloud Availability 3.5



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	What Is vCloud Availability and How Does It Work	4
2	vCloud Availability Administration in the Cloud	7
	Certificates Management	7
	Replacing vCloud Availability Certificates	7
	Replacing External Infrastructure Certificates	16
	Manage the Accessible Provider VDCs	18
	Managing Connections Between Cloud Sites	19
	Pair Cloud Sites	19
	Re-Pair Cloud Sites	21
	Unpair Cloud Sites	22
	Managing Public Administrative Access to vCloud Availability	23
	Allow Public Administrative Access to vCloud Availability	23
	Restrict Public Administrative Access to vCloud Availability	24
	Collecting vCloud Availability Reports	25
	Collect a vCloud Availability Replication Usage Report	25
	Collect a vCloud Availability Storage Consumption Report	27
	Maintenance	29
	Evacuate the Replication Data from a Datastore	29
	vCloud Availability Replicator Maintenance Mode	30
	Rebalance Replications	32
	Troubleshooting	33
	vCloud Availability Operational Verification	33
	Restart the vCloud Availability Services	34
	Unable to Access the vCloud Availability Portal Through vCloud Director	36
	Allow SSH Access	37
	How Do You Collect Support Bundles	37
	How Do You Set Additional Logging Level	39
	How Do You Free Up vCloud Availability Appliance Disk Space	40
3	VMware vCloud Availability Administration On-Premises	42
	Re-Pair On-Premises with Cloud Site	42
	Unpair Cloud Site from On-Premises	43
	Unregister the vCloud Availability vSphere Client Plug-In	44

What Is vCloud Availability and How Does It Work



VMware vCloud Availability provides replications and failover at a vApp or virtual machine level. vCloud Availability is a unified solution, that provides on premises to cloud and cloud to cloud onboarding, migration, and disaster recovery for multi-tenant cloud sites.

What is vCloud Availability

vCloud Availability offers secure migration and disaster recovery capabilities to or between multi-tenant cloud sites. vCloud Availability provides simplified onboarding and ensures the continuous availability of VMware vSphere® workloads and automates recovery operations.

vCloud Availability 3.0 provides VMware Cloud Provider partners with a converged way to protect and recover workloads and data and to provide flexible workload migration services to and from on-premises resources and between cloud sites.

vCloud Availability is a converged appliance-based solution that provides the following capabilities:

- Dedicated interfaces for the services deployment and management
- Native integration with VMware vCloud Director by using the vCloud Director plug-in for the replication management
- Access for tenant and cloud provider users by using the vCloud Availability Portal
- Access for tenant users by using the vCloud Availability vSphere Client Plug-In
- Tenant self-service protection, failover, and failback operations for each virtual machine or for each vApp
- Symmetrical replication and recovery flow that can be started from either the source or the recovery site
- Storage independence from VMware vSphere®

Replication and migration features provided by vCloud Availability:

- Full onboarding and migration capabilities from a single administration interface
- Automated inventory collection of virtual data centers, unprotected and protected vApps and virtual machines, storage profiles, and network configuration

- Self-service virtual machine migration from on-premises resources to cloud, cloud to on-premises resources, or cloud to cloud vApp, and virtual machine migrations between vCloud Director instances
- Managed onboarding and disaster recovery capabilities for on-premises resources to cloud, and cloud to cloud scenarios
- Automated tenant replication, migration, failover, and failback of vApps and operations after a failover

vCloud Availability integration with vCloud Director forms a disaster recovery infrastructure in which the disaster recovery organization controls operate as an activation-controlled policy that provides the disaster recovery capabilities for each tenant. The organization controls include Recovery Point Objective (RPO), snapshots, and number of permitted replications for the tenant disaster recovery.

Service level agreement (SLA) provided by vCloud Availability:

- 5 minutes of minimum RPO
- The RPO is customizable by the cloud provider

Security features provided by vCloud Availability:

- Encryption of the replication traffic by using end-to-end TLS encryption
- Built-in optional compression of the replication traffic
- Built-in vSphere encryption for the stored data

Day-2 cloud provider operations and monitoring of vCloud Availability:

- Policy-based management of the disaster recovery capabilities
- Migration of tenants from one vCloud Director instance to another, for example, to set up a new data center
- Temporary transfer of workloads to another vCloud Director site, for example, to perform maintenance
- Certificate management and password management in the vCloud Availability services and in the disaster recovery infrastructure

Clustering support:

- Cluster datastore support that allows the storage migration to a cluster datastore
- Edge clusters support in vCloud Director ensures an optimal performance of the vCloud Director environments

How Does vCloud Availability Work

In a cloud environment, vCloud Availability Replicator, vCloud Availability Replication Manager, vCloud Availability vApp Replication Manager, and vCloud Availability Tunnel operate together to support the replication management, secure communication, and storage of the replicated data. Cloud providers can support recovery for multiple tenant environments that can scale to handle increasing loads for each tenant and for multiple tenants.

In an on-premises environment, vCloud Availability Replicator and a preconfigured instance of vCloud Availability Tunnel support replication management by using both the vCloud Availability vSphere Client Plug-In and the vCloud Availability Portal, dedicated to tenants.

For more information, go to the [vCloud Availability documentation](#) and the [vCloud Availability product pages](#).

vCloud Availability Administration in the Cloud

2

After installing and configuring vCloud Availability, the service provider can perform management and administrative tasks. These tasks include changes to the provisioned environment and routine administration and maintenance procedures.

This chapter includes the following topics:

- [Certificates Management](#)
- [Manage the Accessible Provider VDCs](#)
- [Managing Connections Between Cloud Sites](#)
- [Managing Public Administrative Access to vCloud Availability](#)
- [Collecting vCloud Availability Reports](#)
- [Maintenance](#)
- [Troubleshooting](#)

Certificates Management

When the SSL certificates are about to expire, the service provider can renew or replace the certificates of the vCloud Availability services and the certificates in the remaining disaster recovery infrastructure.

Replacing vCloud Availability Certificates

Each vCloud Availability service uses a unique SSL certificate both for the HTTPS access to the service management interface and in the communication with other services. After renewing or replacing the certificate of a vCloud Availability service, configure vCloud Availability to trust the certificate.

In a typical cloud deployment, the vCloud Availability solution comprises of three types of appliances with vCloud Availability services:

- Cloud Replication Management appliances that run the vCloud Availability vApp Replication Manager service and vCloud Availability Replication Manager service.
- Cloud Replicator appliances that run the vCloud Availability Replicator service.
- Cloud Tunnel appliances that run the vCloud Availability Tunnel service.

vCloud Availability Tunnel effectively proxies the tenants communication with vCloud Availability vApp Replication Manager. When connecting through the remote vCloud Availability Tunnel, the on-premises appliance sees only the remote vCloud Availability vApp Replication Manager certificate and the tenants do not see the remote vCloud Availability Replicator, vCloud Availability Tunnel, or vCloud Availability Replicator certificates.

Each vCloud Availability service must have a unique certificate which is different from other services certificates. By default, the certificate is self-signed, or you can use a Certificate Authority (CA)-signed certificate. A minimum requirement for the trusted communication is to install a trusted CA-signed certificate only on vCloud Availability vApp Replication Manager, while the other services can continue to use self-signed certificates:

- Use a CA-signed certificate for the vCloud Availability vApp Replication Manager service. On the same Cloud Replication Management appliance, you must use a self-signed certificate for the vCloud Availability Replicator service.
- Use self-signed certificates for vCloud Availability Tunnel and vCloud Availability Replicator. If the disaster recovery environment requires using only public certificates, you can also use CA-signed certificates for these two services.

Using a Wildcard Certificate

You can use a wildcard certificate only for the vCloud Availability vApp Replication Manager service. To keep the certificates unique, you must use self-signed certificates for the remaining vCloud Availability services. Do not use the same wildcard certificate for more than one cloud site.

Managing the vCloud Availability Certificates

Certificates are part of the communication chain used to validate the hosts and are also used for the vCloud Availability services management interfaces. To renew or to replace the certificates, you can import a CA-signed certificate or regenerate the self-signed certificate for each VMware vCloud Availability service.

Regenerate a Self-Signed Certificate

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

Procedure

- 1 Log in to the vCloud Availability management interface.
 - a In a web browser, go to **https://Appliance-IP-address/ui/admin**.
 - b Select **SSO login** or **Appliance login**, and enter the single sign-on or the **root** user credentials.
 - c Click **Login**.
- 2 In the left pane, click **Configuration**.
- 3 Under **Appliance settings**, next to **Certificate** click **Regenerate**.
- 4 In the **Regenerate Certificate** window, click **Apply**.

Results

After the certificate is regenerated, all vCloud Availability services that run on the same appliance restart.

What to do next

You can find the old certificate at `/opt/vmware/h4/serviceType/config/keystore.p12.bak`, where *serviceType* is **c**loud, **m**anager, **r**eplicator, or **t**unnel.

Upload a CA-Signed Certificate

To prevent the Web browser from showing a certificate prompt every time a user opens the vCloud Availability interface, you must upload an SSL certificate signed by a trusted certificate authority.

Prerequisites

- Verify that the new PKCS#12 (PFX) certificate file and the private key use the same password.
- Verify that the PKCS#12 file contains only one entry: the private key and its corresponding certificate and, optionally, the certificate trust chain. The trust chain must be part of the same keystore entry and must not be provided as separate entries in the PKCS#12 file.
- Verify that the RSA key size is 2048-bit or larger.
- Verify that the certificate does not use insecure hash algorithms, for example SHA1 and MD5.
- If using a wildcard certificate, use it only for the vCloud Availability vApp Replication Manager service. Do not use the same certificate for any other vCloud Availability service. For more information about wildcard certificates, see [Replacing vCloud Availability Certificates](#).

Procedure

- 1 Log in to the vCloud Availability service management interface.
 - a In a Web browser, go to **`https://Appliance-IP-address/ui/admin`**.
 - b Select **SSO login** or **Appliance login**, and enter the single sign-on or the **root** user credentials.
 - c Click **Login**.
- 2 In the left pane, click **Configuration**.
- 3 Under **Appliance settings**, next to **Certificate** click **Import**.
- 4 In the **Import Certificate** window, enter the certificate details and click **Apply**.
 - a Enter the password that protects the keystore and the certificate private key.
 - b Click **Browse** and select the PKCS#12 file.

Results

After you upload the CA-signed certificate, all vCloud Availability services that run on the same appliance restart.

What to do next

You can find the old certificate at `/opt/vmware/h4/service type/config/keystore.p12.bkp`, where *service type* is `cloud`, `manager`, `replicator`, or `tunnel`.

Replace the vCloud Availability vApp Replication Manager Certificate

Regenerate the vCloud Availability vApp Replication Manager self-signed SSL certificate or import a CA-signed certificate. With the new certificate, reestablish the trust with the local vCloud Availability Tunnel and re-pair all cloud sites.

Replacing the vCloud Availability vApp Replication Manager certificate invalidates the trust with both the local and the remote vCloud Availability Tunnel services and the paired cloud sites. Reestablish the trust with the local vCloud Availability Tunnel service and re-pair the cloud sites.

Procedure

- 1 Log in to the management interface of the vCloud Availability Cloud Replication Management Appliance.
 - a In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.
- 2 Replace the vCloud Availability vApp Replication Manager certificate.
 - a In the left pane, click **Configuration**.
 - b Under **Appliance settings** next to **Certificate**, select the certificate replacement method.

Option	Description
Import	Upload a CA-signed certificate.
Regenerate	Generate a new self-signed certificate.

- c Click **Apply**.

vCloud Availability vApp Replication Manager creates a copy of the old certificate at `/opt/vmware/h4/cloud/config/keystore.p12.bak`. You are logged out and the services automatically restart in a few minutes.
- 3 Log in to the management interface of the vCloud Availability Cloud Replication Management Appliance.
 - a In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.

- 4 Trust the new vCloud Availability vApp Replication Manager certificate in the vCloud Availability Tunnel service.
 - a In the left pane, click **Configuration**.
 - b Under **Service endpoints**, next to **Tunnel address** click **Edit**.
 - c In the **Tunneling Settings** window, enter the vCloud Availability Tunnel **root** user credentials and click **Apply**.
 - d To complete the trust reestablishment, accept the local vCloud Availability Tunnel SSL certificate.
- 5 Trust the new vCloud Availability vApp Replication Manager certificate in the paired cloud sites.
 - a In the left pane, click **Sites**.
 - b Select a cloud site and click **Repair**.
 - c In the **Update Pairing** window, select **Remote appliance credentials**.
 - d Enter the remote vCloud Availability vApp Replication Manager **root** user password and click **Update**.
 - e To complete the trust reestablishment, accept the remote vCloud Availability vApp Replication Manager SSL certificate.

Note Repeat this step and select to re-pair the remaining cloud sites.

What to do next

Re-pair all on-premises sites with the local site. For more information, see [Re-Pair On-Premises with Cloud Site](#).

Replace the vCloud Availability Replication Manager Certificate

Regenerate the vCloud Availability Replication Manager self-signed SSL certificate or import a CA-signed certificate. With the new certificate, reestablish the trust with the vCloud Availability Replicator services and re-pair all cloud sites.

Replacing the certificate of the vCloud Availability Replication Manager service invalidates the trust between all vCloud Availability Replicator services in the local, remote cloud, and remote on-premises sites. To reestablish the trust, re-pair the registration of vCloud Availability Replicator services in the remote site and re-pair the cloud sites.

Important After re-pairing the cloud sites, you must manually re-pair all on-premises sites. To configure the vCloud Availability on-premises appliance, see the *Installing and Configuring vCloud Availability On-Premises* document.

Procedure

- 1 Log in to the vCloud Availability Replication Manager service management interface.
 - a In a Web browser, go to `https://Appliance-IP-Address:8441/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.

- 2 Replace the vCloud Availability Replication Manager certificate.
 - a In the left pane, click **Configuration**.
 - b Under **Appliance settings** next to **Certificate**, select the certificate replacement method.

Option	Description
Import	Upload a CA-signed certificate.
Regenerate	Generate a new self-signed certificate.

- c Click **Apply**.
vCloud Availability Replication Manager creates a copy of the old certificate at `/opt/vmware/h4/cloud/config/keystore.p12.bak`. You are logged out and the services automatically restart in a few minutes.
- 3 Log in to the vCloud Availability Replication Manager service management interface.
 - a In a Web browser, go to `https://Appliance-IP-Address:8441/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.
- 4 Trust the new vCloud Availability Replication Manager certificate in the local vCloud Availability Replicator instance.
 - a In the left pane, click **Replicators**.
 - b On the **Replicators administration** page, select the local vCloud Availability Replicator instance and click **Repair**.
 - c In the **Details for replicator** window, enter the Cloud Replication Management appliance **root** user password, the single sign-on credentials and click **Apply**.
 - d To complete the trust reestablishment, accept the vCloud Availability Replicator SSL certificate.

Note Repeat this step and to trust the new certificate select the remaining vCloud Availability Replicator instances.

- 5 Log in to the management interface of the vCloud Availability Cloud Replication Management Appliance.
 - a In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.
- 6 Trust the new vCloud Availability Replication Manager certificate in the paired cloud sites.
 - a In the left pane, click **Sites**.
 - b Select a cloud site and click **Repair**.
 - c In the **Update Pairing** window, keep **Remote appliance credentials** enabled.
 - d Enter the remote vCloud Availability vApp Replication Manager **root** user password and click **Update**.
 - e To complete the trust reestablishment, accept the remote vCloud Availability vApp Replication Manager SSL certificate.

Note Repeat this step and to re-pair select the remaining cloud sites.

What to do next

Re-pair all on-premises sites with the local site. For more information, see [Re-Pair On-Premises with Cloud Site](#).

Replace the vCloud Availability Replicator Certificate

When the certificate of the vCloud Availability Replicator service expires, you must replace it with the new self-signed or CA-signed certificate.

Replacing the SSL certificate of the vCloud Availability Replicator unregisters it from the vCloud Availability Replication Manager in the local and in the remote sites. To repair the registration of the vCloud Availability Replicator to the vCloud Availability Replication Manager in the remote site, you must re-establish the trust between the cloud sites. For more information, see [Re-Pair Cloud Sites](#).

Prerequisites

Verify that you are prepared to follow the steps in these procedures when replacing the certificate:

- [Regenerate a Self-Signed Certificate](#) or [Upload a CA-Signed Certificate](#).

Procedure

- 1 In a Web browser, go to the vCloud Availability Replicator service management interface for your deployment type.

Deployment type	Service Management Interface
vCloud Availability Combined Appliance	https://Appliance-IP-Address:8440/ui/admin
vCloud Availability Cloud Replicator Appliance	https://Replicator-Appliance-IP-Address/ui/admin

- a Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - b Click **Login**.
- 2 Log in as **root**.
 - 3 Generate or upload a new certificate.
 - 4 Re-pair the registration of vCloud Availability Replicator instances to the vCloud Availability Replication Manager service on the local site.

- a Log in again to the vCloud Availability Replication Manager service management interface at <https://Replication-Manager-IP-address:8441/ui/admin>.

On the **System Monitoring** tab all vCloud Availability Replicator instances are **Offline**.

- b On the **Replicators** tab, select a vCloud Availability Replicator instance and click **Repair**.
- c Enter the 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 name that has administrative privileges for the local site single sign-on domain, for example <i>Administrator@VSPHERE.LOCAL</i> .
SSO Password	The password for the administrative user.

- d Accept the SSL certificate of the vCloud Availability Replicator service.
 - e Repeat steps b to d 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 on the **System Monitoring** tab.
- 5 In the service management interface of the vCloud Availability vApp Replication Manager appliance, navigate to the **Sites** tab.
 - 6 Select a cloud site and click **Repair**.

Note You must perform this step for each cloud site.

Replace the vCloud Availability Tunnel Certificate

When the certificate of the vCloud Availability Tunnel service expires, you must replace it with a new self-signed or a CA-signed certificate.

Replace the certificate of the vCloud Availability Tunnel only in cloud sites.

Prerequisites

Verify that you are prepared to follow the steps in these procedures when replacing the certificate:

- [Regenerate a Self-Signed Certificate](#)
- [Upload a CA-Signed Certificate](#)

Procedure

- 1 In a Web browser, go to the vCloud Availability Tunnel service management interface for your deployment type.

Deployment type	Service Management Interface
vCloud Availability Combined Appliance	<code>https://Appliance-IP-Address:8442/ui/admin</code>
vCloud Availability Cloud Tunnel Appliance	<code>https://Tunnel-Appliance-IP-Address/ui/admin</code>

- a Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - b Click **Login**.
- 2 Log in as **root**.
 - 3 Generate or upload a new certificate.
 - 4 Log in to the management interface of the vCloud Availability Cloud Replication Management Appliance.
 - a In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.
 - 5 In the left pane, click **Configuration** and next to **Tunnel address** click **Edit**.
 - 6 In the **Tunneling settings** window, click **Apply**.
 - 7 Verify the thumbprint and accept the new vCloud Availability Tunnel SSL certificate.

Results

After replacing the certificate of the vCloud Availability Tunnel, on-premises and cloud sites might initially show a Generic error occurred during TLS handshake message for this vCloud Availability Tunnel

instance connectivity. Without further actions, within 30 minutes vCloud Availability negotiates the certificate and restores the connectivity.

Replacing External Infrastructure Certificates

After renewing or replacing the SSL certificate of the vCenter Server Lookup service on a Platform Services Controller or changing the vCloud Director endpoint or its certificate, you must configure the vCloud Availability services to work with the new certificate.

Configure vCloud Availability to Accept a Renewed vCloud Director Endpoint or Certificate

After changing the vCloud Director endpoint or renewing its SSL certificate, configure vCloud Availability to trust the new certificate and communicate with vCloud Director.

Skip this procedure, if vCloud Availability is configured to discover the vCloud Director service address automatically.

Prerequisites

Verify that the SSL certificate of vCloud Director is successfully renewed. For information about generating and importing SSL certificates in vCloud Director, see [VMware KB 1026309](#).

Procedure

- 1 Log in to the vCloud Availability service management interface.
 - a In a Web browser, go to **`https://Appliance-IP-address/ui/admin`**.
 - b Select **SSO login** or **Appliance login**, and enter the **single sign-on** or the **root** user credentials.
 - c Click **Login**.
- 2 In the left pane, click **Configuration**.
- 3 Under **Service endpoints**, next to **vCloud Director address** click **Edit**.
- 4 On the **vCloud Director Details** page, click **Apply**.
- 5 Verify that the details of the certificate are correct, and click **Accept**.
- 6 In the left pane, click **System Monitoring**.
- 7 Under **System health**, click **Restart service**.

Configure vCloud Availability to Accept a Renewed vCenter Server Lookup service Certificate

After renewing the vCenter Server Lookup service certificate on a Platform Services Controller instance that is used as a replication or a migration source or destination, you must configure the vCloud Availability components to trust the renewed certificate.

Prerequisites

- Verify that the SSL certificate of the Platform Services Controller certificate is successfully renewed, and that the vCenter Server Lookup service is updated to use the renewed certificate. For information about replacing the SSL certificate on a Platform Services Controller, see [VMware KB 2118939](#).
- Verify that all components in your environment that depend on the vCenter Server registration in the vCenter Server Lookup service are configured to trust the renewed certificate. An example of such a component is NSX Manager.

Procedure

- 1 Configure the vCloud Availability Replicator to work with the renewed Platform Services Controller certificate.

If you are using dedicated vCloud Availability Replicator appliances, repeat this step for all vCloud Availability Replicator instances.

- a In a Web browser, go to the vCloud Availability Replicator service management interface at **`https://Replicator-Appliance-IP:8440/ui/admin`**.
- b Log in as the **root** user.
- c In the left pane, click **Configuration**.
- d Under **Service endpoints**, next to **Lookup service address** click **Edit**.
- e In the **Lookup Service Details** dialog box, enter the vCenter Server Lookup service address and click **Apply**.
The details of the renewed vCenter Server Lookup service certificate appear.
- f To complete the vCloud Availability Replicator configuration, accept the renewed vCenter Server Lookup service certificate.

- 2 Configure the vCloud Availability Replication Manager to work with the renewed Platform Services Controller certificate.

- a In a Web browser, go to the vCloud Availability Replication Manager service management interface at **`https://Replication-Manager-IP-address:8441/ui/admin`**.
- b Log in as the **root** user.
- c In the left pane, click **Configuration**.
- d Under **Service endpoints**, next to **Lookup service address** click **Edit**.
- e In the **Lookup Service Details** dialog box, enter the Lookup service address and click **Apply**.
The details of the renewed vCenter Server Lookup service certificate appear.
- f To complete the vCloud Availability Replication Manager configuration, accept the renewed vCenter Server Lookup service certificate.

- 3 Configure the vCloud Availability vApp Replication Manager to work with the renewed Platform Services Controller certificate.
 - a In a Web browser, go to the vCloud Availability vApp Replication Manager service management interface at **`https://vApp-Replication-Manager-IP-address/ui/admin`**.
 - b Log in as the **root** user.
 - c In the left pane, click **Configuration**.
 - d Under **Service endpoints**, next to **Lookup service address** click **Edit**.
 - e In the **Lookup Service Details** dialog box, enter the Lookup service address and click **Apply**.
The details of the renewed vCenter Server Lookup service certificate appear.
 - f To complete the vCloud Availability vApp Replication Manager configuration, accept the renewed vCenter Server Lookup service certificate.

- 4 If you are using a single sign-on login to vCloud Availability Tunnel, configure the vCloud Availability Tunnel to work with the renewed Platform Services Controller certificate.
If you are using dedicated vCloud Availability Tunnel appliances, repeat this step for all vCloud Availability Tunnel instances.
 - a In a Web browser, go to the vCloud Availability Tunnel service management interface at **`https://Tunnel-Appliance-IP:8442/ui/admin`**.
 - b Log in as the **root** user.
 - c In the left pane, click **Configuration**.
 - d Under **Service endpoints**, next to **Lookup service address** click **Edit**.
 - e In the **Lookup Service Details** dialog box, enter the Lookup service address and click **Apply**.
The details of the renewed vCenter Server Lookup service certificate appear.
 - f To complete the vCloud Availability Tunnel configuration, accept the renewed vCenter Server Lookup service certificate.

Manage the Accessible Provider VDCs

By default, vCloud Availability has access to all provider virtual data centers (VDCs) managed by the vCloud Director instance. Each vCloud Availability instance allows the service provider to manage the accessible provider VDCs.

Procedure

- 1 Log in to the management interface of the vCloud Availability Cloud Replication Management Appliance.
 - a In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.
- 2 In the left pane, click **Configuration**.
- 3 Under **Site details**, next to **Accessible Provider VDCs**, click **Edit**.
- 4 In the **Accessible Provider VDCs** windows, select **vCloud Availability can access the following Provider VDCs** and enable the provider VDCs that this vCloud Availability instance can access.
vCloud Availability now limits the visible inventory objects in replication wizards to this selection of provider VDCs.

What to do next

You can create replications only by using inventory objects that belong to the selected provider VDCs.

Managing Connections Between Cloud Sites

Cloud sites management includes establishing and re-establishing trust between sites. After you initiate pairing from the local site and complete the pairing from the remote site, vCloud Availability establishes a trust between the two cloud sites. Re-establish the trust after upgrading vCloud Availability, after replacing the vCloud Availability vApp Replication Manager certificate, or after registering additional vCloud Availability Replicator instances.

Pair Cloud Sites

To initiate a trust establishment between two cloud sites with vCloud Availability instances, you initiate pairing from either of the two sites. Depending on the vCloud Availability versions in the sites, to complete establishing the trust, you perform the pairing procedure in the local and the remote sites or only in the local site.

Depending on the version of vCloud Availability in the cloud sites, use the appropriate pairing process:

- To pair site A and site B, both running vCloud Availability 3.5, perform the procedure from both sites:
 - a From site A, initiate the pairing process with site B.
 - b From site B, complete the pairing process with site A.
- To pair a site running vCloud Availability 3.5 and a site running vCloud Availability 3.0.x, perform the following steps:
 - a In the vCloud Availability 3.5 site, allow the administrative access from public IPs. For more information, see [Allow Public Administrative Access to vCloud Availability](#).

- b In the vCloud Availability 3.0.x site, initiate and complete the pairing process with the vCloud Availability 3.5 site.

When pairing from the vCloud Availability 3.0.x site, you must provide the password of the **root** user of the remote site vCloud Availability Cloud Replicator Appliance. For more information, see [Pair Cloud Sites](#) in *Administering vCloud Availability 3.0*.

- c In the vCloud Availability 3.5 site, after completing the pairing process, disallow the administrative access from public IPs. For more information, see [Allow Public Administrative Access to vCloud Availability](#).
- To pair site A and site B, both running vCloud Availability 3.0.x, see [Pair Cloud Sites](#) in *Administering vCloud Availability 3.0*.

Prerequisites

Verify that the vCloud Availability appliances are configured in both cloud sites:

- vCloud Availability Cloud Replication Management Appliance
- vCloud Availability Cloud Replicator Appliance(s)
- vCloud Availability Cloud Tunnel Appliance

Procedure

- 1 Log in to the management interface of the vCloud Availability Cloud Replication Management Appliance.
 - a In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.
- 2 In the left pane, click **Sites**.
- 3 On the **Cloud sites** page, click **New Pairing**.
- 4 In the **New Pairing** window, configure the connection to the cloud site, and to initiate the trust between the two sites click **Pair**.

Option	Description
Site name	Provide an exact match of the remote cloud site name.
Endpoint URL	Enter the external Endpoint URL of the remote site. For port, you can use the external DNAT-ed port (443 by default) and if the vCloud Availability Tunnels are internally visible between both sites, you might use the internal address and port of the vCloud Availability Tunnel:8048. For example, <code>https://remote-vcda.provider.com:443</code> .
Description	Optionally provide a description for the cloud site pair.

- 5 To complete the first half of the pair process, accept the remote vCloud Availability vApp Replication Manager SSL certificate.

vCloud Availability initiates the trust between the two sites.

- 6 To complete the pairing, log in to the remote cloud site and pair with the local site by repeating this procedure.

vCloud Availability establishes the trust between the two sites.

- 7 On the **Cloud sites** page, verify that the new cloud site is listed and does not show any errors.

What to do next

You can configure new replications, after modifying the default replication policy for both the source and for the destination organization to allow replications. Alternatively, a custom replication policy that is assigned to the source and to the destination organizations must allow replications. For information about the replication policy, see [Configuring Replication Policies](#) in *Using vCloud Availability*.

Re-Pair Cloud Sites

After you register a vCloud Availability Replicator, replace the vCloud Availability vApp Replication Manager certificate, or upgrade vCloud Availability in the local site, go to each paired remote site and re-pair each remote site with the local site.

Depending on the version of vCloud Availability in the cloud sites, use the appropriate re-pairing process:

- To re-pair a site running vCloud Availability 3.5 and a site running vCloud Availability 3.0.x:
 - a In the vCloud Availability 3.5 site, allow the administrative access from public IPs.
 - b In the vCloud Availability 3.0.x site, initiate and complete the re-pairing process with the vCloud Availability 3.5 site.
 - c In the vCloud Availability 3.5 site, disallow the administrative access from public IPs.
- To re-pair site A and site B, running vCloud Availability 3.5:
 - a From site A, initiate the re-pairing process with site B.
 - b From site B, to complete the re-pairing process, re-pair with site A.

Prerequisites

- If both sites are running vCloud Availability 3.0.x, to re-pair a cloud site you must allow the administrative access from public IPs only during pairing. For more information, see [Allow Public Administrative Access to vCloud Availability](#).

Procedure

- 1 Log in to the management interface of the vCloud Availability Cloud Replication Management Appliance.
 - a In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.
- 2 In the left pane, click **Sites**.
- 3 On the **Cloud sites** page, click **Repair**.
- 4 In the **Update Pairing** window, configure the connection to the cloud site and click **Update**.

Option	Description
Endpoint URL	Verify that the displayed IP address of the vCloud Availability Tunnel appliance in the remote site is correct.
Description	Optionally provide a description for the cloud site pair.

- 5 To complete the re-pair process, accept the remote vCloud Availability vApp Replication Manager SSL certificate.
The trust between the two sites is successfully reestablished.
- 6 If you are running vCloud Availability 3.0.1, restart the vCloud Availability vApp Replication Manager services at both cloud sites.
- 7 On the **Cloud sites** page, verify that the site is listed without errors.

Results

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

What to do next

If you are running vCloud Availability 3.0.1 or later, revert the administrative access from public IPs after re-pairing cloud sites. For more information, see [Restrict Public Administrative Access to vCloud Availability](#).

Unpair Cloud Sites

To remove the established trust between vCloud Availability and a cloud site, unpair the cloud site from the vCloud Availability appliance.

Prerequisites

Delete all configured replications with the cloud site.

Procedure

- 1 Log in to the management interface of the vCloud Availability Cloud Replication Management Appliance.
 - a In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.
- 2 In the left pane, click **Configuration**.
- 3 In the **Pairing** section, click **Unpair**.
- 4 In the **Unpair from cloud site** dialog box, enter the vCloud Director organization **administrator** credentials and click **Apply**.

Results

The pairing with the cloud site is removed.

What to do next

You can remove the established connection between the on-premises appliance and vCenter Server. See [Unregister the vCloud Availability vSphere Client Plug-In](#).

Managing Public Administrative Access to vCloud Availability

Introduced in vCloud Availability 3.0.1, in a dedicated appliance deployment, administrative sessions to all vCloud Availability services are restricted by default when originating from public networks.

The restriction applies to the following administrative accounts:

- Login sessions by using the appliance **root** user credentials
- Login sessions by using vCloud Director **system administrator** credentials
- Login sessions by using a single sign-on user with vCenter Server **Administrator** credentials

When vCloud Availability restricts the external administrative access, attempts to establish a login session from a public IP result in a 401 Not Authenticated response, which is identical to a wrong password error. To improve the appliance security further, the appliance denies the external administrative login session without counting it as an unsuccessful login attempt.

Allow Public Administrative Access to vCloud Availability

In a dedicated appliance deployment, administrative sessions from public IPs are restricted to all vCloud Availability services. If you need external administrative access, you can allow administrative sessions from public IP addresses.

Prerequisites

Procedure

- 1 Log in to the management interface of the vCloud Availability Cloud Replication Management Appliance.
 - a In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.
- 2 In the left pane, click **Configuration**.
- 3 Under **Security settings**, next to **Restrict Admin APIs by source IP**, click **Edit**.
- 4 In the **Restrict Admin APIs by source IP** window, select **Allow admin access from anywhere** and click **Apply**.

Under **Security settings**, next to **Restrict Admin APIs by source IP**, you see `Allow admin access from anywhere` listed.

Results

The external administrative sessions to all vCloud Availability services are enabled.

What to do next

Revert the restriction after completing the external administrative operation. For more information, see [Restrict Public Administrative Access to vCloud Availability](#).

Restrict Public Administrative Access to vCloud Availability

If you have enabled administrative access from public IPs, to improve the security you revert the restriction to its default value.

Prerequisites

Procedure

- 1 Log in to the management interface of the vCloud Availability Cloud Replication Management Appliance.
 - a In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.
- 2 In the left pane, click **Configuration**.
- 3 Under **Security settings**, next to **Restrict Admin APIs by source IP** click **Edit**.

- 4 In the **Restrict Admin APIs by source IP** window, select **Do not allow admin sessions from the Internet (recommended)** and click **Apply**.

Under **Security settings**, next to **Restrict Admin APIs by source IP** you can see Do not allow admin sessions from the Internet listed.

Results

The administrative sessions from public IPs to all vCloud Availability services are restricted.

Collecting vCloud Availability Reports

You can extract a report containing data with the replication usage or with the storage consumption of vCloud Availability.

Collect a vCloud Availability Replication Usage Report

Extract the incoming replication usage data from vCloud Availability. The report contains the number of incoming replications and the number of incoming replications aggregated by organizations and by virtual data centers.

Procedure

- 1 Connect to the vCloud Availability vApp Replication Manager appliance by using a Secure Shell (SSH) client.
 - a Open an SSH connection to *Appliance-IP-Address*.
 - b Log in as the **root** user.
- 2 Obtain a vCloud Availability vApp Replication Manager token.

```
$ c4 loginroot 'vApp-Replication-Manager-Password'
```

```
[
  "token-id",
  {
    "user": "root",
    "roles": [
      "EVERYONE",
      "ADMINISTRATORS",
      "VRADMINISTRATORS"
    ],
    "authenticatedSites": [
      { "site": "site1", "org": "System" }
    ]
  }
]
```

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

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

4 Generate the vCloud Availability usage report.

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

By not using the `--dry-run` argument, the usage report overwrites the reporting data in the two `.tsv` files.

The `/tmp/report_summary.tsv` file contains the number of all incoming replications and information about incoming replications grouped by organizations and by virtual data centers. This information is presented in the following format:

```
vCloud Availability Usage Report
generatedOn date-time-stamp
buildVersion 3.x-build-number
localSite site1
instanceId instance-id

Incoming replication counts
Replication type Total count Cloud to cloud protections Cloud to cloud migrations vSphere to
cloud protections vSphere to cloud migrations
Total incoming vApp replications 5 1 0 3 1
Newly started incoming vApp replications 5 1 0 3 1
Carried over incoming vApp replications 0 0 0 0 0
Total incoming VM replications 5 1 0 3 1
Newly started incoming VM replications 5 1 0 3 1
Carried over incoming VM replications 0 0 0 0 0

Incoming vApp replications by org
Org Org Id Total count Cloud to cloud protections Cloud to cloud migrations vSphere to cloud
protections vSphere to cloud migrations
alpha eb410797-9038-4755-a7f1-f28981ef5408 2 1 0 1 0
beta 082ce1a1-7b17-4316-92ab-db82da0c35e0 3 0 0 2 1

Incoming VM replications by org
Org Org Id Total count Cloud to cloud protections Cloud to cloud migrations vSphere to cloud
protections vSphere to cloud migrations
alpha eb410797-9038-4755-a7f1-f28981ef5408 2 1 0 1 0
beta 082ce1a1-7b17-4316-92ab-db82da0c35e0 3 0 0 2 1

Incoming vApp replications by vDC
vDC vDC Id Org Total count Cloud to cloud protections Cloud to cloud migrations vSphere to cloud
protections vSphere to cloud migrations
alphaorgvdc1 33ff6729-b55f-4ae8-bf20-6b0b553542ed alpha 2 1 0 1 0
betaorgvdc1 964ce5f9-e8b9-494c-81dd-4deea158b61e beta 3 0 0 2 1

Incoming VM replications by vDC
vDC vDC Id Org Total count Cloud to cloud protections Cloud to cloud migrations vSphere to cloud
protections vSphere to cloud migrations
alphaorgvdc1 33ff6729-b55f-4ae8-bf20-6b0b553542ed alpha 2 1 0 1 0
betaorgvdc1 964ce5f9-e8b9-494c-81dd-4deea158b61e beta 3 0 0 2 1
```

```

End of report.
vCloud Availability Detailed Usage Report
generatedOn 2019-09-10 10:55:42.359126
buildVersion 3.5.0.14556251-71017ba
localSite site1
instanceId cb45ee35-09b8-4c80-b72a-0c0d4290e924

Incoming replication counts
Replication type Total count Cloud to cloud protections Cloud to cloud migrations vSphere to
cloud protections vSphere to cloud migrations
Total incoming vApp replications 5 1 0 3 1
Newly started incoming vApp replications 5 1 0 3 1
Carried over incoming vApp replications 0 0 0 0 0
Total incoming VM replications 5 1 0 3 1
Newly started incoming VM replications 5 1 0 3 1
Carried over incoming VM replications 0 0 0 0 0

Incoming VM Replications
Replication Type Migration/Protection 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
Destination vDC Id Destination vDC
cloud-to-cloud protection ...
vsphere-to-cloud protection ...
vsphere-to-cloud protection ...
vsphere-to-cloud migration ...
vsphere-to-cloud protection ...

End of report.

```

- 5 Download the vCloud Availability usage report to your local machine.

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

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

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

Collect a vCloud Availability Storage Consumption Report

You can extract the storage consumption data from vCloud Availability. Start by creating daily snapshots that aggregate a detailed report with the monthly storage consumption. At the end of the reporting period, generate an aggregated report containing the average storage consumption.

Procedure

- 1 Connect to the vCloud Availability vApp Replication Manager appliance by using a Secure Shell (SSH) client.
 - a Open an SSH connection to *Appliance-IP-Address*.
 - b Log in as the **root** user.

2 Obtain a vCloud Availability vApp Replication Manager token.

```
$ c4 loginroot 'vApp-Replication-Manager-Password'
```

```
[
  "token-id",
  {
    "user": "root",
    "roles": [
      "EVERYONE",
      "ADMINISTRATORS",
      "VRADMINISTRATORS"
    ],
    "authenticatedSites": [
      { "site": "site1", "org": "System" }
    ]
  }
]
```

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

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

4 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 - snapshot Storage Consumption Report

generatedOn    date time stamp
productName    vSphere Replication Cloud (C4)
buildVersion   vCloud.Availability.version-build
localSite      site2
instanceId     instance-id

Storage consumption by org
Org  Org Id  Storage consumed      Number of PITs
s20rg  c6415681-9456-4051-88bd-5b3ebf75f610  10486784  0

Storage consumption by vDC
vDC  vDC Id  Org  Storage consumed      Number of PITs
vdc_s20rg  f5aed876-4d62-4c35-9d3d-9c3065a8bcfb  s20rg  10486784  0

# End of report.
```

5 Generate the vCloud Availability storage consumption report.

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

Each run of the `storage-report` script deletes all snapshots of the previously created reports. Run the `storage-report` script at the end of a reporting period to aggregate storage snapshots for the ending reporting period and prepare for the next reporting period.

The aggregated storage consumption report is in the following format:

```
# vCloud Availability - aggregated Storage Consumption Report

generatedOn    date-time-stamp
productName    vSphere Replication Cloud (C4)
buildVersion   3.x-build-number
localSite      site2
instanceId     instance-id

Storage consumption by org (avg)
Org    Org Id  Storage consumed    Number of PITs
s20rg  c6415681-9456-4051-88bd-5b3ebf75f610    10486784    0

Storage consumption by vDC (avg)
vDC    vDC Id  Org    Storage consumed    Number of PITs
vdc_s20rg    f5aed876-4d62-4c35-9d3d-9c3065a8bcfb    s20rg    10486784    0

# End of report.
```

- Download the vCloud Availability storage consumption report to your local machine.

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

- (Optional) Remove the generated instance of the report from the vCloud Availability vApp Replication Manager appliance.

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

Maintenance

Perform maintenance operations on a datastore or on a vCloud Availability Replicator instance and rebalance replications across vCloud Availability Replicator instances.

Evacuate the Replication Data from a Datastore

To perform maintenance operations on a local datastore in the cloud site, you must first remove all incoming replications and replication data placed on that datastore. To evacuate the replications from the datastore at once, you apply an alternative storage policy to all incoming replications on the datastore.

- Evacuating a datastore might take several hours to complete and depends on the amount of data to be transferred.
- Evacuating datastore clusters is not supported. Such datastores are not listed, even when used as the replications destination storage policy.

Prerequisites

Verify that vCloud Availability 3.5 is deployed in the cloud site.

Procedure

- 1 Log in to the management interface of the vCloud Availability Cloud Replication Management Appliance.
 - a In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.
- 2 In the left pane, click **Datastores**.
- 3 To see a filter showing the replications that are placed on the highlighted datastore, click **Preview**.
- 4 Select a local datastore that lists a replications counter and click **Evacuate**.
- 5 In the **Evacuate datastore** window, select the destination storage policy for all incoming replications residing on the datastore and click **Apply**.
 - **Reset current storage policy** apply the current storage policy to each matching replication. After removing or adding datastores to the storage policy, this option can move the replication replica files, to make the matching replications compliant with their storage policy.
 - **Any** store all the replications to all the shared datastores to which the Any storage policy is applied.
 - **pVDC Storage policy** apply the selected storage policy to all matching replications. If the *pVDC Storage policy* is not exposed to a tenant data center, the replications of this tenant remain placed on the datastore.

Results

vCloud Availability applies the selected storage policy and starts evacuating the incoming replications and replica files from the selected local datastore in the cloud site.

What to do next

You can track the progress of the Change storage profiles task by clicking **System Tasks** in the left pane.

vCloud Availability Replicator Maintenance Mode

To prepare a vCloud Availability Replicator instance for maintenance without disrupting replications, you can evacuate the incoming replications from the vCloud Availability Replicator instance to other local vCloud Availability Replicator instances in the cloud site.

The vCloud Availability Replicator instance must be placed in maintenance mode in each site where it is registered. This procedure is a two-step process, performed first in the local site, then repeated in the remote sites:

- 1 In the local site, placing the vCloud Availability Replicator instance in maintenance mode migrates all incoming cloud replications to other vCloud Availability Replicator instances in the local site. Also, vCloud Availability migrates all incoming and outgoing replications from and to on-premises sites.
- 2 In the remote site, migrate the remaining outgoing cloud replications from this vCloud Availability Replicator instance to other vCloud Availability Replicator instances. Log in to the remote site and place in maintenance mode the same vCloud Availability Replicator instance. Repeat this step in each remote site, where this vCloud Availability Replicator instance is remotely registered.

New replications are placed on vCloud Availability Replicator instances that are not in maintenance mode.

Prerequisites

- Verify that vCloud Availability 3.5 is deployed in the cloud site.
- Verify that more than one vCloud Availability Replicator instance is operational in the cloud site.
- Verify that the clean-up task is complete after using a test failover for any incoming replication. If vCloud Availability Replicator contains a test failed over virtual machine, attempting to enter a maintenance mode shows a *Operation aborted due to an unexpected error* message. Before entering maintenance mode, you must perform a test cleanup on the test failed over virtual machine or vApp.

Procedure

- 1 Log in to the vCloud Availability Replication Manager service management interface.
 - a In a Web browser, go to `https://Appliance-IP-Address:8441/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.
- 2 In the left pane, click **Replicators**.
- 3 To evacuate the incoming replications, select the local vCloud Availability Replicator instance and click **Enter Maintenance Mode**.
- 4 To evacuate the outgoing replications from this vCloud Availability Replicator instance, log in to the vCloud Availability Replication Manager in the remote site and repeat this procedure.

In the remote site, select the same vCloud Availability Replicator instance that is remotely registered. Repeat step 4 for all cloud sites, where the vCloud Availability Replicator instance is remotely registered.

Results

After placing a vCloud Availability Replicator instance in maintenance mode from both the local site and all remote sites where it is registered, vCloud Availability evacuates all replications from that vCloud

Availability Replicator instance. The vCloud Availability Replicator instance is ready for maintenance operations.

What to do next

After performing the maintenance operations, in the local site click **Exit Maintenance Mode**. To repopulate the vCloud Availability Replicator instance with replications, you must rebalance the replications. For more information, see [Rebalance Replications](#).

Rebalance Replications

To distribute the incoming replications evenly over all vCloud Availability Replicator instances in the site, you can rebalance the replications.

vCloud Availability assigns all new replications to the vCloud Availability Replicator with the fewest number of replications in the site. After adding an extra vCloud Availability Replicator instance, vCloud Availability assigns all new replications to the new vCloud Availability Replicator instance. Replications that existed before adding the new vCloud Availability Replicator instance remain assigned to the previous vCloud Availability Replicator instances. The result is an unequal balance of the number of replications per vCloud Availability Replicator instance. You can see how many replications are assigned to each vCloud Availability Replicator instance and rebalance the replications. This operation migrates the replications from vCloud Availability Replicator instances with more replications to vCloud Availability Replicator instances with fewer replications.

Prerequisites

- Verify that vCloud Availability 3.5 is deployed in the site.
- Verify that more than one vCloud Availability Replicator instance is operational in the site.

Procedure

- 1 Log in to the vCloud Availability Replication Manager service management interface.
 - a In a Web browser, go to `https://Appliance-IP-Address:8441/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.
- 2 In the left pane, click **Replicators**.
- 3 To rebalance the replications, click **Rebalance**.
- 4 In the **Rebalance Site** window, select a site to rebalance and click **Apply**.

Repeat step 4 for all paired sites.

Results

vCloud Availability migrates and evenly distributes the replications to each operational vCloud Availability Replicator instance in the site.

Troubleshooting

In the disaster recovery environment, you can diagnose and correct problems related to vCloud Availability services operation, logging, and others.

vCloud Availability Operational Verification

After deploying vCloud Availability, verify that all services are correctly running by logging in to each service management interface and validating the service connectivity status.

Prerequisites

Verify that vCloud Availability is successfully deployed and powered on.

Procedure

- 1 Verify that the vCloud Availability vApp Replication Manager instance is operational.
 - a Open a Web browser and go to **`https://Appliance-IP-Address/ui/admin`**.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the single sign-on user credentials.
 - c Click **Login**.
 - d In the left pane, click **System Monitoring**.
 - e In the **Service status** section, verify that all connectivity checks report a green check icon.
- 2 Verify that the vCloud Availability Replication Manager instance is operational.
 - a Open a Web browser and go to **`https://Appliance-IP-Address:8441/ui/admin`**.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the single sign-on user credentials.
 - c Click **Login**.
 - d In the left pane, click **System Monitoring**.
 - e In the **Service status** section, verify that all connectivity checks report a green check icon.
- 3 Verify that the vCloud Availability Replicator instances are operational.
 - a Open a Web browser and go to the management endpoint for your deployment type.

Deployment type	Management Endpoint
Combined Appliance	<code>https://Appliance-IP-Address:8440/ui/admin</code>
Cloud Replicator Appliance	<code>https://Replicator-Appliance-IP-Address/ui/admin</code>

- b Log in as the **root** user.
- c In the left pane, click **System Monitoring**.
- d In the **Service status** section, verify that all connectivity checks report a green check icon.

- 4 Verify that the vCloud Availability Tunnel instances are operational.
 - a Open a Web browser and go to the management endpoint for your deployment type.

Deployment type	Management Endpoint
Combined Appliance	<code>https://Appliance-IP-Address:8442/ui/admin</code>
Cloud Tunnel Appliance	<code>https://Tunnel-Appliance-IP-Address/ui/admin</code>

- b Log in as the **root** user.
- c In the left pane, click **System Monitoring**.
- d In the **Service status** section, verify that all connectivity checks report a green check icon.

Results

As a result, you can successfully authenticate to each management endpoint and validate that each vCloud Availability service is operational.

What to do next

To start creating and managing replications, access one of the following interfaces:

- In the on-premises vSphere Client, authenticate with the single sign-on administrator credentials and access the vCloud Availability vSphere Client Plug-In. For more information, see *Accessing the vCloud Availability vSphere Client Plug-In* in the *Using vCloud Availability* documentation.
- Go to the vCloud Availability Portal and log in as the vCloud Director organization administrator.

Restart the vCloud Availability Services

As part of the troubleshooting, you can restart all vCloud Availability services in a combined appliance from the **System Monitoring** page. To restart the services that are in dedicated appliances, log in to the management interface of each appliance.

Depending on the vCloud Availability appliance deployment type, you restart the services in a specific order. After restarting each service, wait a couple of minutes for the service to become operational and display its service management interface again.

Procedure

- 1 Log in to the management interface of the vCloud Availability Cloud Replication Management Appliance.
 - a In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.

2 Restart the vCloud Availability vApp Replication Manager and the vCloud Availability Replication Manager service.

- a In the left pane, click **System Monitoring**.
- b Under **System health**, click **Restart service**.
- c In the **Restart service** window, confirm the restart operation by clicking **Restart**.

3 In a Web browser, go to the vCloud Availability Replicator service management interface for your deployment type.

Deployment type	Service Management Interface
vCloud Availability Combined Appliance	https://Appliance-IP-Address:8440/ui/admin
vCloud Availability Cloud Replicator Appliance	https://Replicator-Appliance-IP-Address/ui/admin

- a Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
- b Click **Login**.

4 Restart the vCloud Availability Replicator service.

- a In the left pane, click **System Monitoring**.
- b Under **System health**, click **Restart service**.
- c In the **Restart service** window, confirm the service restart by clicking **Restart**.

5 In a Web browser, go to the vCloud Availability Tunnel service management interface for your deployment type.

Deployment type	Service Management Interface
vCloud Availability Combined Appliance	https://Appliance-IP-Address:8442/ui/admin
vCloud Availability Cloud Tunnel Appliance	https://Tunnel-Appliance-IP-Address/ui/admin

- a Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
- b Click **Login**.

6 Restart the vCloud Availability Tunnel service.

- a In the left pane, click **System Monitoring**.
- b Under **System health**, click **Restart service**.
- c In the **Restart service** window, confirm the service restart by clicking **Restart**.

Unable to Access the vCloud Availability Portal Through vCloud Director

You are unable to access the vCloud Availability 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 in the **vCloud Director Tenant Portal**, or clicking it does not open the vCloud Availability Portal.
- In the vCloud Availability logs, you see the Unable to register vCAV plugin in vCD error.

Cause

Connectivity problems during the initial configuration of vCloud Availability might prevent the vCloud Availability plug-in from registering with vCloud Director.

Solution

- 1 Log in to the vCloud Availability Portal.
 - a Open a Web browser and go to **`https://vApp-Replication-Manager-IP-address/ui/admin`**.
 - b Log in as the **root** user.
- 2 Re-register the vCloud Availability plug-in with vCloud Director.
 - a On the **Configuration** tab, next to the **vCloud Director address** click **Edit**.
 - b Select the configuration type and click **Apply**.
 - If you select **Discover the vCloud Director Service address automatically**, proceed directly to [Step Step 3](#).
 - If you select **Enter details for the vCloud Director Service manually**, proceed with [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"> ■ VMware vCloud Director is federated with a previously specified Lookup service. ■ There is only one registered VMware vCloud Director in the Lookup service. ■ The single sign-on user belongs to the System administrator group in VMware vCloud Director.
Enter details for the vCloud Director Service manually	Select this option, if your VMware vCloud Director instance is not federated with a previously specified Lookup service or if multiple VMware vCloud Director instances are registered with 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.

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

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

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

Allow SSH Access

vCloud Availability does not allow Secure Shell (SSH) access by default. To connect to the vCloud Availability appliance by using an SSH client, first you must allow the SSH access in the management interface.

Prerequisites

Verify that vCloud Availability 3.5 is deployed.

Procedure

- 1 Log in to the management interface of the vCloud Availability Cloud Replication Management Appliance.
 - a In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.
- 2 In the left pane, click **Configuration**.
- 3 Under **Security settings** and next to **Allow SSH access**, click **Edit**.
- 4 In the **Allow SSH access** window, select **Allow SSH access** and click **Apply**.

Results

The vCloud Availability appliance now allows SSH connections.

What to do next

You can connect to the vCloud Availability appliance by using an SSH client.

How Do You Collect Support Bundles

For troubleshooting purposes, VMware Technical Support might request support bundles. For each product, you can collect the diagnostic information in a support bundle by using a specific user interface, method, script, or tool. The support bundle contains product-specific logs, configuration files, and data appropriate to the situation.

Use case: an issue with vCloud Availability requires troubleshooting by using a support bundle. You can collect relevant support bundles for each vCloud Availability component and for the disaster recovery environment components such as vCloud Director and vCenter Server.

Procedure

- 1 Collect a support bundle for the vCloud Availability components by using the service management interface.

- a In a Web browser, go to the management interface for each vCloud Availability component.

Deployment type	Component	Management Interface
vCloud Availability Combined Appliance	vCloud Availability vApp Replication Manager	https://Appliance-IP-Address/ui/admin
	vCloud Availability Replication Manager	https://Appliance-IP-Address:8441/ui/admin
	vCloud Availability Replicator	https://Appliance-IP-Address:8440/ui/admin
	vCloud Availability Tunnel	https://Appliance-IP-Address:8442/ui/admin
vCloud Availability Cloud Replicator Appliance	vCloud Availability Replicator	https://Replicator-Appliance-IP-Address/ui/admin
vCloud Availability Cloud Tunnel Appliance	vCloud Availability Tunnel	https://Tunnel-Appliance-IP-Address/ui/admin

- b Log in as the **root** user.
- c In the left pane, click **Support**.
- d On the **Support bundles** page, click **Generate new**.
- e In the **Bundle generate** window, initiate the creation of a support bundle by clicking **Generate**.
- f After the support bundle is generated, in the **Bundle Id** column, initiate a download by clicking the **bundle id** link.
- g In the **Download Support Bundle** window, save the support bundle file locally by clicking **Download**.
- h After your browser downloads the file, optionally select the bundle and click **Delete**.

- 2 If you cannot access the vCloud Availability service management interface, collect a support bundle by using a Secure Shell (SSH) client.

- a Open an SSH connection to the *vCloud-Availability-Appliance-IP-Address* virtual machine and log in by using the **root** user credentials.
- b Create a folder for the support bundle.

```
mkdir bundles
```

- c Generate the support bundle by running the `/opt/vmware/h4/bin/support-bundle.py` script and providing arguments with the deployment type of the appliance and the output folder.

In a combined appliance deployment type, the following example collects all logs.

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

In a dedicated appliance deployment type, you can open an SSH connection to each vCloud Availability appliance and run the script providing the respective deployment type as argument.

- d Download the `/root/bundles/bundle-YYYY-MM-DD_HH-mm-SS-Time-Zone/combined-bundle-YYYY-MM-DD_HH-mm-SS-Time-Zone.tar.bz2` file.

- 3 Collect a vCloud Director support bundle by using a Secure Shell (SSH) client.

- a Open an SSH connection to the *vCloud-Director-IP-Address* virtual machine and log in by using your user credentials.
- b Generate the support bundle file.

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

- c Download the `vmware-vcd-support-YYYY-MM-DD.NNNN.tgz` support bundle file from `/opt/vmware/vcloud-director/data/transfer/vmware-vcd-support`.

- 4 Collect a vCenter Server support bundle by using the user interface.

- a In a Web browser, go to **`https://vCenter-Server-FQDN:443/appliance/support-bundle`**.
- b Log in by using the **root** user credentials, and click **Enter** to start the download.

Results

After downloading the support bundles, you can provide them to VMware Technical Support.

How Do You Set Additional Logging Level

To perform additional troubleshooting, increase the logging level. Use the vCloud Availability management interface and set the logging level for each service.

Use case: after exhausting the logs, you might need an extra level of logging detail. To generate the additional level of logging data, configure each vCloud Availability component.

Procedure

- 1 Log in to the management interface of the vCloud Availability Cloud Replication Management Appliance.
 - a In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
 - b Select **Appliance login** or **SSO login** and enter the **root** or the *single sign-on* user credentials.
 - c Click **Login**.
- 2 In the left pane, click **Configuration**.
- 3 Under **Appliance settings** next to **Logging levels**, click **Edit**.
- 4 In the **Edit Log Levels** window, for each service you can set the logging level from **Off** to **All**.
- 5 To apply the configuration, click **Apply**.
The modified logging level persists until the service restarts.
- 6 Connect to the vCloud Availability appliance by using a Secure Shell (SSH) client.
 - a Open an SSH connection to *Appliance-IP-Address*.
 - b Authenticate as the **root** user.
- 7 See the vCloud Availability services log files.

vCloud Availability Service	Service Log File Location
vCloud Availability Replication Manager	<code>/opt/vmware/h4/manager/log/manager.log</code>
vCloud Availability Replicator	<code>/opt/vmware/h4/replicator/log/replicator.log</code>
vCloud Availability vApp Replication Manager	<code>/opt/vmware/h4/cloud/log/cloud.log</code>
vCloud Availability Tunnel	<code>/opt/vmware/h4/tunnel/log/tunnel.log</code>

How Do You Free Up vCloud Availability Appliance Disk Space

If the available appliance disk space is low, you can remove obsolete or unnecessary files.

Use case: you can regularly clean up the appliance disk space after using advanced troubleshooting or if the disk space is low.

Procedure

- 1 Clear the vCloud Availability appliance service logs.
 - a Connect to the vCloud Availability appliance by using a Secure Shell (SSH) client and authenticate as the **root** user.
 - b Navigate to the following folders and remove the service logs that are old or unnecessary.
 - /opt/vmware/h4/cloud/log
 - /opt/vmware/h4/manager/log
 - /opt/vmware/h4/replicator/log
 - /opt/vmware/h4/tunnel/log
- 2 Clear the vCloud Availability appliance support bundles.
 - a In a Web browser, go to **https://Appliance-IP-Address/ui/admin** and log in as the **root** user or as a single sign on user.
 - b In the left pane, click **Support** and delete all unnecessary support bundles.
 - c Log in to the vCloud Availability appliance by using a Secure Shell (SSH) client and authenticate as the **root** user.
 - d Navigate to the following folders and remove the support bundles that are not available under the **Support bundles** page.
 - /opt/vmware/h4/cloud/support
 - /opt/vmware/h4/manager/support
 - /opt/vmware/h4/replicator/support
 - /opt/vmware/h4/tunnel/support
- 3 If you have a dedicated Cloud Replicator appliance, remove the core dumps.
 - a Connect to the Cloud Replicator appliance by using a Secure Shell (SSH) client and authenticate as the **root** user.
 - b Navigate to the /var/core/ folder and remove the HBR core* files.

Results

The available disk space on the vCloud Availability appliance is increased.

What to do next

You can also check the /var/log and the /tmp folders for unnecessary files and delete them.

VMware vCloud Availability Administration On-Premises

3

After installing and configuring the on-premises vCloud Availability appliance, you can re-pair or unpair the cloud sites from the on-premises site and unregister the on-premises vCloud Availability appliance from vCenter Server.

This chapter includes the following topics:

- [Re-Pair On-Premises with Cloud Site](#)
- [Unpair Cloud Site from On-Premises](#)
- [Unregister the vCloud Availability vSphere Client Plug-In](#)

Re-Pair On-Premises with Cloud Site

To reestablish the trust between the on-premises site and a cloud site, you re-pair the cloud site from the on-premises vCloud Availability appliance.

Procedure

- 1 Log in to the management interface of the vCloud Availability On-Premises Appliance.
 - a In a Web browser, go to `https://On-Prem-Appliance-IP-address/ui/admin`.
 - b Log in as the **root** user.
- 2 In the left pane, click **Configuration**.
- 3 In the **Pairing** section, click **Repair**.
- 4 In the **Update Pairing** wizard, reestablish the trust with the cloud site.
 - a On the **Site Details** page, verify the site name and description and click **Next**.
 - b On the **Lookup Service** page, optionally enter the **single sign-on** user credentials and click **Next**.

- c On the **Cloud Details** page, provide tenant credentials to use during pairing and configure access from cloud.

Option	Description
Public API Endpoint	<i>Public-API-Endpoint:8048</i>
Organization Admin	vCloud Director admin@org
Organization Password	vCloud Director <i>organization admin password</i>
Allow Access from Cloud	<p>Select to allow the cloud provider and the organization administrators to perform the following operations from the vCloud Availability Portal without authenticating to the on-premises site:</p> <ul style="list-style-type: none"> ■ Discover on-premises workloads and replicate them to the cloud. ■ Reverse existing replications to the on-premises site. ■ Replicate cloud workloads to the on-premises site. <p>Deselect to only allow users authenticated to the on-premises vCloud Availability Portal to configure new replications and existing replications cannot be reversed from the vCloud Availability Portal.</p>

- d Verify the thumbprint, accept the SSL certificate of the vCloud Availability Public API endpoint and click **Next**.
- e On the **Ready To Complete** page, review the summary details and click **Finish**.
- 5 Verify that the connectivity to the cloud site is operational.
- a In the left pane, click **System Monitoring**.
- b Under **Cloud Status**, verify that for the cloud site you re-paired, **Service connectivity** shows a green OK status.

Results

The pairing between the on-premises site and the cloud site is re-established.

Unpair Cloud Site from On-Premises

To remove the established trust between the on-premises site and the cloud site, from the vCloud Availability On-Premises Appliance you can unpair the cloud site.

Prerequisites

- Delete all configured replications between the on-premises site and the cloud site.

Procedure

- 1 Log in to the management interface of the vCloud Availability On-Premises Appliance.
 - a In a Web browser, go to `https://On-Prem-Appliance-IP-address/ui/admin`.
 - b Log in as the **root** user.
- 2 In the left pane, click **Configuration**.

- 3 Under **Site details**, next to **Pairing** click **Unpair**.
- 4 In the **Unpair from cloud site** window, enter the vCloud Director organization **administrator** credentials and click **Apply**.

The **Pairing** section shows Not configured and the cloud site is removed from the vCloud Availability On-Premises Appliance.

Results

The pairing between the on-premises site and the cloud site is removed.

What to do next

- You can remove the established connection between the on-premises appliance and vCenter Server, see [Unregister the vCloud Availability vSphere Client Plug-In](#).
- You can pair the on-premises appliance and the cloud vCloud Availability Replicator again, from the on-premises site, see [Re-Pair On-Premises with Cloud Site](#).

Unregister the vCloud Availability vSphere Client Plug-In

To remove the established connection between the vCloud Availability On-Premises Appliance and the on-premises vCenter Server, you remove the vCenter Server Lookup service from the vCloud Availability On-Premises Appliance.

Procedure

- 1 Log in to the management interface of the vCloud Availability On-Premises Appliance.
 - a In a Web browser, go to `https://On-Prem-Appliance-IP-address/ui/admin`.
 - b Log in as the **root** user.
- 2 In the left pane, click **Configuration**.
- 3 Under **Service endpoints**, next to **Lookup Service Address** click **Remove**.
- 4 In the **Remove Lookup Service Registration** window, enter the single sign-on **administrator** credentials and click **Remove**.

The vCenter Server Lookup service is unregistered from the vCloud Availability On-Premises Appliance configuration. After you log out and log in to vCenter Server, you can see that the vCloud Availability vSphere Client Plug-In is unregistered from the on-premises vCenter Server.

Results

The vCloud Availability On-Premises Appliance is ready to be configured with the vCenter Server Lookup service and allows running the initial setup wizard.

What to do next

You can use the on-premises vCloud Availability appliance again, after running the initial setup wizard. If the on-premises site is still paired with a cloud site, use the same vCenter Server Lookup service as in the configuration before the pairing.