Administration Guide

24 NOV 2022

VMware Cloud Director Availability 4.5

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

https://docs.vmware.com/

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

Contents

Administration Guide

1

VMware Cloud Director Availability™ provides replications and failover at a vApp or virtual machine level. VMware Cloud Director 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 VMware Cloud Director Availability

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

VMware Cloud Director Availability 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.

VMware Cloud Director Availability is a converged appliance-based solution that provides the following capabilities:

- Dedicated interfaces for the services deployment and management.
- For cloud sites backed by VMware Cloud Director™, VMware Cloud Director Availability offers native integration with VMware Cloud Director by using the VMware Cloud Director plug-in.
- Access for on-premises users by using the VMware Cloud Director 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 vSphere.

Replication and migration features provided by VMware Cloud Director Availability:

- Full onboarding and migration capabilities from a single management 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 sites.
- 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.

When VMware Cloud Director Availability integrates with VMware Cloud Director, it 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 for replications with sites backed by VMware Cloud Director:

- 1 minute of minimum RPO.
- The RPO is customizable by the cloud provider.

Security features provided by VMware Cloud Director Availability:

- Encryption of the replication traffic by using end-to-end TLS encryption.
- The TLS session is terminated at each Replicator Appliance.
- Built-in optional compression of the replication traffic.

Day-2 operations and monitoring of VMware Cloud Director Availability:

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

How Does VMware Cloud Director Availability Work

- In a cloud site backed by VMware Cloud Director, Replicator Service instances, a Manager Service, a Cloud Service, and a Tunnel Service operate together to support the replication management, secure communication, and storage of the replicated data. The providers can support recovery for multiple tenant environments that can scale to handle increasing loads for each tenant and for multiple tenants.
- In a cloud vCenter Server site, a Replicator Service, a Manager Service, and a Tunnel Service operate in a vCenter Replication Management Appliance.

- In an on-premises site, Replicator Service and a preconfigured instance of Tunnel Service operating in either depending on the remote cloud site:
  - an On-Premises to Cloud Director Replication Appliance, or in
  - an On-Premises to Cloud vCenter Replication Appliance,

  support replication management by using both the VMware Cloud Director Availability vSphere Client Plug-In and the VMware Cloud Director Availability Tenant Portal, dedicated to tenants.

For more information, go to the VMware Cloud Director Availability documentation and the VMware Cloud Director Availability product pages.

Administration in the Cloud Director Site

2

After installing and configuring VMware Cloud Director Availability in the cloud site backed by VMware Cloud Director, you can perform management and administrative tasks. The following tasks include changes to the provisioned environment and routine administration and maintenance procedures.

- **Cloud site backed by VMware Cloud Director:**

  In a VMware Cloud Director Availability cloud site, backed by VMware Cloud Director, perform the following administration tasks in this current chapter by using the appliances management interface or in the disaster recovery infrastructure.

- **On-premises and Provider vCenter Server site:**

  For information about VMware Cloud Director Availability in vCenter Server sites, see the Chapter 3 Administration in On-Premises and Provider Site chapter.

This chapter includes the following topics:

Activate Data Engine for Replications

As a **provider**, to replicate workloads between two sites, activate the supported data engines for starting new replications, depending on the source and the destination sites.

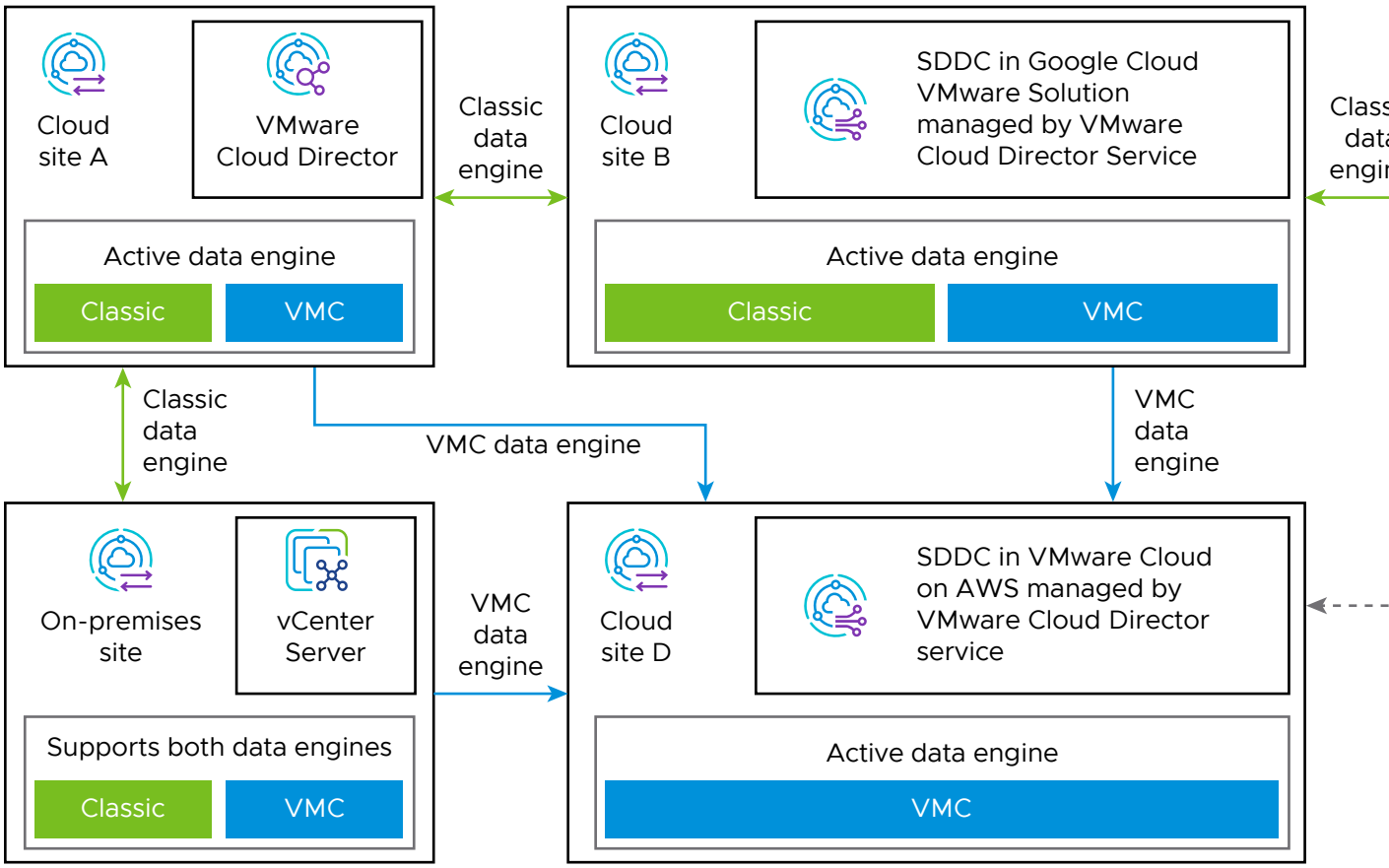
Important For information about the supported data engines, depending on the source and the destination site, see Replications use cases.

At a replication start, VMware Cloud Director Availability checks whether the currently active data engines match between the source and the destination site:

- If both data engines are activated in both sites, then the **Classic** data engine takes precedence.
- If no available data engine matches between both sites, then the replication fails. In the following example diagram, only **Classic** data engine is active in the source site (Cloud site C) and only **VMC** is active in the destination site (Cloud site D) as is the only supported data engine for this site.

For example, in the following diagram the arrows indicate the replication direction and the used data engine:

Figure 2-1. Activated data engines for replications between supported sites



Note Already started replications remain operational regardless of the active data engines. Activating a data engine affects only the start of new replications.

Deactivating a data engine that is used for replications which are already started, has no effect on them.

Prerequisites

- Verify that for activating the **VMC** data engine, VMware Cloud Director Availability 4.2 or later is successfully deployed in the site, as earlier versions only support the **Classic** data engine.
- Verify that all the required network ports are open in the firewalls. For information about the required open ports, see: VMware Ports and Protocols, or Deployment Requirements On-Premises and Network Requirements.

Procedure

1 Log in to the management interface of the Cloud Director Replication Management Appliance.
   a In a Web browser, go to `https://Cloud-Director-Replication-Management-Appliance-IP-Address/ui/admin`.
   b Select **Appliance login** and enter the **root** user password.
   c Click **Login**.
2 In the left pane under **Configuration**, click **Settings**.
3 Under **Site settings**, next to **Data engine** click **Edit**.
   a In the **Data engine** window, activate one or both data engines for replications:
      - **Classic** - supports both migrations and protections.
      - **VMC** - supports only migrations.
   b Click **Apply**.

   The activated data engine in this site becomes available for handling new replications.

What to do next

Once activated in both sites, you can create new replications that use this data engine between the two sites.

Managing Pairing with Cloud Director Sites

The pairing management includes establishing and re-establishing trust with cloud sites backed by VMware Cloud Director. After you initiate pairing from the local site and complete the pairing from the remote site, VMware Cloud Director Availability establishes a trust between the two sites. Re-establish the trust after upgrading VMware Cloud Director Availability, after replacing the Cloud Service certificate, or after registering additional Replicator Service instances.

Remember As a **provider** you must add each Cloud Service instance or each vCenter Replication Management Appliance for metering in VMware vCloud® Usage Meter before creating any replications. For information about adding the cloud sites in vCloud Usage Meter, see vCloud Usage Meter Integration.

Pairing Interoperability with Mismatching VMware Cloud Director Availability Versions

You can pair sites that have different VMware Cloud Director Availability major versions deployed, up to two major versions back, or `(N-2)`, where `N` is the currently deployed version.

For example, you can pair a site where version 4.5 is running with a site where version 4.3 or later is running, but not with a site where version 4.2 or earlier is running. Mismatching site versions can occur when upgrading the sites one at a time, or when migrating workloads from earlier vSphere and VMware Cloud Director versions to a site with later vSphere and VMware Cloud Director versions.

Note When pairing sites with different VMware Cloud Director Availability major versions, only the functionality of the earlier version is supported.

For example, only the functionality and features of VMware Cloud Director Availability 4.3 are supported when pairing a site where version 4.3 is running with a site where version 4.5 is running.

Before pairing VMware Cloud Director Availability sites, verify the interoperability of the versions of VMware Cloud Director Availability between the source site and the destination site in the following tables:

Table 2-1. Pairing Interoperability Between the Version of On-Premises to Cloud Director Replication Appliance the Version of the VMware Cloud Director Availability in the Cloud Director Site

On-Premises to Cloud Director Replication Appliance	Cloud Site 3.0	Cloud Site 3.5	Cloud Site 4.0	Cloud Site 4.1	Cloud Site 4.2	Cloud Site 4.3	Cloud Site 4.4	Cloud Site 4.5
3.0	Supported	Supported	Supported	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported
3.5	Supported	Supported	Supported	Supported	Unsupported	Unsupported	Unsupported	Unsupported
4.0	Supported	Supported	Supported	Supported	Supported	Unsupported	Unsupported	Unsupported
4.1	Unsupported	Supported	Supported	Supported	Supported	Supported	Unsupported	Unsupported
4.2	Unsupported	Unsupported	Supported	Supported	Supported	Supported	Supported	Unsupported
4.3	Unsupported	Unsupported	Unsupported	Supported	Supported	Supported	Supported	Supported
4.4	Unsupported	Unsupported	Unsupported	Unsupported	Supported	Supported	Supported	Supported
4.5	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported	Supported	Supported	Supported

Note Do not pair sites with more than two major versions apart.

For example, pairing version 4.5 with version 4.3 is supported but pairing version 4.5 with version 4.2 is not supported.

Table 2-2. Pairing Interoperability Between the Version of VMware Cloud Director Availability in the Source Cloud Director Site and the Version of the VMware Cloud Director Availability in the Destination Cloud Director Site

Source Cloud Site VMware Cloud Director Availability	Destination Cloud Site 3.0	Destination Cloud Site 3.5	Destination Cloud Site 4.0	Destination Cloud Site 4.1	Destination Cloud Site 4.2	Destination Cloud Site 4.3	Destination Cloud Site 4.4	Destination Cloud Site 4.5
3.0	Supported	Supported	Supported	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported
3.5	Supported	Supported	Supported	Supported	Unsupported	Unsupported	Unsupported	Unsupported
4.0	Supported	Supported	Supported	Supported	Supported	Unsupported	Unsupported	Unsupported
4.1	Unsupported	Supported	Supported	Supported	Supported	Supported	Unsupported	Unsupported
4.2	Unsupported	Unsupported	Supported	Supported	Supported	Supported	Supported	Unsupported
4.3	Unsupported	Unsupported	Unsupported	Supported	Supported	Supported	Supported	Supported
4.4	Unsupported	Unsupported	Unsupported	Unsupported	Supported	Supported	Supported	Supported
4.5	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported	Supported	Supported	Supported

Important When pairing sites, ensure that the latest maintenance patch release for the VMware Cloud Director Availability major version is deployed in each site.

- **Latest release:**

  For each major version bellow, see the latest available release that must be deployed before pairing each site:

  - For version 3.0, the site must be running version 3.0.5 or if later is available.
  - For version 3.5, the site must be running version 3.5.2 or if later is available.
  - For version 4.0, the site must be running version 4.0.1.2 or if later is available.
  - For version 4.1, the site must be running version 4.1.1 or if later is available.
  - For version 4.2, the site must be running version 4.2.1 or if later is available.
  - For version 4.3, the site must be running version 4.3.1 or if later is available.
  - For version 4.4, the site must be running version 4.4.1 or if later is available.

- **Supported versions:**

  For a list of the currently supported VMware Cloud Director Availability versions, see the below link in Supported Versions.

Migrating from Earlier VMware Cloud Director Availability Versions

By pairing an earlier and later VMware Cloud Director Availability versions, you can migrate workloads from source sites where the later VMware Cloud Director Availability version does not support either the version of vCenter Server or VMware Cloud Director.

VMware Cloud Director Availability is fully capable of migrating workloads running on earlier vSphere and VMware Cloud Director versions that are near or are already EOS. If there is a VMware Cloud Director Availability version compatible with the vSphere and the VMware Cloud Director versions in the source site, you can pair it to VMware Cloud Director Availability 4.0 deployed in a cloud site with later vSphere and VMware Cloud Director versions. For example, see the following table:

Table 2-3. Migration Interoperability with Paired Sites with Earlier VMware Cloud Director Availability Versions

Migration Source Site Early Version	Migration Destination Site Latest Supported Version
On-premises site A, deployed version 3.5 with vSphere 5.5 or later.	Cloud site C, VMware Cloud Director Availability 4.1* with a supported VMware Cloud Director version**.
Cloud site B, deployed version 3.5 with vCloud Director 9.0 or 9.1.	
Cloud site Y, deployed version 3.0 with vCloud Director 8.2, 9.0 or 9.1.	Cloud site Z, VMware Cloud Director Availability 4.0* with a supported VMware Cloud Director version**.

Note * Migrating from a site running earlier version requires a specific version of VMware Cloud Director Availability in the destination site, that may not be the latest currently available, due to the pairing interoperability. For information about the pairing interoperability between the different VMware Cloud Director Availability versions, see the tables in the top section.

- For example, in an on-premises site with vSphere 5.5, deploy an on-premises appliance version 3.5 and pair it to VMware Cloud Director Availability 4.1 deployed in a cloud site with a supported VMware Cloud Director version**. You can then migrate all virtual machines to the later cloud site.
- For example, in a cloud site with vCloud Director 9.0, deploy version 3.0 and pair it to VMware Cloud Director Availability 4.0 deployed in a cloud site with a supported VMware Cloud Director version**. You can then migrate all vApps to the later VMware Cloud Director site.

Supported Versions

For the currently supported VMware Cloud Director Availability versions, see the VMware Cloud Director Availability Documentation page.

VMware Cloud Director Availability Interoperability Matrices

** Before deploying VMware Cloud Director Availability in the cloud site, verify the supported versions of VMware Cloud Director and NSX by following the link below.

Before deploying On-Premises to Cloud Director Replication Appliance, verify the supported versions of vCenter Server, ESXi, and NSX by following the link below.

For information about the VMware Cloud Director Availability interoperability with other VMware products, see the VMware Product Interoperability Matrix.

Pair cloud sites backed by VMware Cloud Director

To initiate a trust establishment between two cloud sites running VMware Cloud Director Availability instances, initiate pairing from either of the two sites. Then, to complete establishing the trust, repeat the pairing procedure in the remote site.

To pair site A and site B, repeat the steps twice and perform the pairing procedure in both cloud sites:

1 In cloud site A, initiate pairing with a remote cloud site B.

2 In cloud site B, complete pairing with site A.

Prerequisites

- Verify that, before pairing sites, the versions of VMware Cloud Director Availability in both sites can interoperate together. For the pairing interoperability, see Managing Pairing with Cloud Director Sites.
- Verify that in both cloud sites, all the VMware Cloud Director Availability appliances are successfully configured:
  - Cloud Director Replication Management Appliance
  - Replicator Appliance instances
  - Tunnel Appliance

Procedure

1 Log in to the management interface of the Cloud Director 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 under **Configuration**, click **Peer Sites**.

3 On the **Peer Sites** page, click **New cloud pairing**.

4 In the **New Cloud Pairing** window, configure the pairing with the remote cloud site, and to initiate the trust between the local and the remote cloud sites click **Pair**.

Option	Description
Site name	Enter a local site name, exactly matching the remote cloud site name.
Service Endpoint	Enter the public URL of the Service Endpoint, external for the remote cloud site. ■ For the network port, enter the externally DNAT-ed port, by default port 443. ■ If both Tunnel Service instances are internally visible between the two cloud sites, you can enter the internal URL or private IP address of the Tunnel Service and enter port 8048 for direct communication. For example, enter `https://remote-vcda.provider.com:443`.
Description	Optionally, enter a description for the paired cloud site.

5 Complete the first half of the pair process.

a Verify the thumbprint and accept the remote Cloud Service SSL certificate.

b In the **Additional actions** required window, click **OK**.

VMware Cloud Director Availability initiates the trust between the two cloud sites.

Visit the Cloud Service in the *Site name* and complete the pairing operation.

6 To complete the pairing between both sites, log in to the remote cloud site and repeat this procedure for pairing with the local site.

VMware Cloud Director Availability establishes the trust between the two cloud sites.

7 Under **Peer Sites**, verify that the new cloud site is listed and does not show any errors.

8 Before creating any replications, verify that as a **provider** you added each Cloud Service instance for metering in VMware vCloud® Usage Meter.

For information about adding the cloud sites instances in vCloud Usage Meter, see vCloud Usage Meter Integration.

What to do next

After ensuring the Cloud Service instances are metered by vCloud Usage Meter, you can now start creating and managing replications. 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 the *User Guide*.

Re-pair cloud sites backed by VMware Cloud Director

After you register a Replicator Service instance, replace the Cloud Service certificate, or upgrade VMware Cloud Director Availability in the local site, go to each paired remote site and re-pair each remote site with the local site.

To re-pair site A with site B, repeat the steps twice and perform the re-pairing procedure in both cloud sites:

1 In cloud site A, initiate re-pairing with a remote cloud site B.

2 In cloud site B, complete re-pairing with site A.

Procedure

1 Log in to the management interface of the Cloud Director 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 under **Configuration**, click **Peer Sites**.

3 In the **Peer Sites** page, select a remote cloud site for repairing with and click **Repair**.

4 In the **Update Pairing** window, verify the pairing settings of the remote site and click **Update**.

Option	Description
Site name	Dimmed, as the site name cannot be changed.
Service Endpoint	Verify that the both the Service Endpoint address and the network port of the remote site Tunnel Appliance are correct.
Description	Optionally, enter a description for the cloud site.

5 To complete the re-pair process, verify the thumbprint and accept the remote Cloud Service SSL certificate.

   The trust between the two sites is successfully reestablished.

6 Under **Peer Sites**, verify that the remote site shows as `Repaired`.

Results

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

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 the *User Guide*.

Unpair paired sites from the cloud backed by VMware Cloud Director

To remove the established trust between a VMware Cloud Director Availability cloud site and a paired site, delete the paired site from the cloud site.

Prerequisites

Verify that all configured replications with the paired site are deleted.

Procedure

1. Log in to the management interface of the Cloud Director 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 under **Configuration**, click **Peer Sites**.
3. Remove the established trust with a cloud site.
   a. In the **Cloud sites** page, select a cloud site and click **Delete**.
   b. In the **Delete Peer Cloud Site** window, to remove the cloud site pairing, click **Delete**.

   You removed the pairing with the cloud site and removed the trust from both the local and the remote cloud sites.
4. Remove the established trust with an on-premises site from the cloud site.
   - If the on-premises site is still paired, now delete the pairing from the cloud site and then from the on-premises site, unpair the cloud site. For information about unpairing from the on-premises site, see Unpair a Site.
   - If from the on-premises site the cloud site is already unpaired, delete the remaining record in the cloud site.

   a. Under **On-premises sites**, click **Delete**.
   b. In the **Delete On-Premises Site** window, to remove the on-premises site pairing, click **Delete**.

      Above **On-premises sites** you see a green `On-Premises site deleted successfully.` message.

   You removed the cloud site trust with the on-premises site. If you performed this procedure from the cloud site first, in the on-premises site the cloud site still shows as paired. For more information, see Unpair a Site.

Managing Public Administrative Access to VMware Cloud Director Availability

By default, VMware Cloud Director Availability restricts the administrative sessions to all services when originating from public networks. As a **service provider**, you can allow the administrative access from public networks.

The restriction applies to the following administrative accounts:

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

With restricted external administrative access, attempting to establish a login session from a public IP results in a `401 Not Authenticated` response. This response 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 VMware Cloud Director Availability

In a dedicated appliance deployment, administrative sessions from public IPs are restricted to all VMware Cloud Director 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 Cloud Director 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 under **Configuration**, click **Settings**.
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 VMware Cloud Director 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 VMware Cloud Director Availability.

Restrict Public Administrative Access to VMware Cloud Director 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 Cloud Director 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 under **Configuration**, click **Settings**.
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 VMware Cloud Director Availability services are restricted.

Manage the Accessible Provider VDCs

By default, VMware Cloud Director Availability can access all provider virtual data centers (VDCs) that the VMware Cloud Director instance manages. As a **service provider**, you can manage the accessible provider VDCs for each VMware Cloud Director Availability instance.

Note In a multi-site deployment when the vCenter Server instances are in separate data centers but in the same SSO domain, the Replicator Service tries connecting to all vCenter Server instances in the SSO domain, even restricted provider VDCs. If this connectivity is not possible to some remote vCenter Server due to network restrictions, navigating to **System Health** in the user interface can be slow and the logs can contain messages about connectivity problems.

Procedure

1. Log in to the management interface of the Cloud Director 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 under **Configuration**, click **Settings**.
3. Under **Site details** next to **Accessible Provider VDCs**, click **Edit**.
4. In the **Accessible Provider VDCs** window, select **VMware Cloud Director Availability can access the following Provider VDCs** and enable the provider VDCs that this VMware Cloud Director Availability instance can access.

   VMware Cloud Director 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.

Certificates Management

In a cloud site backed by VMware Cloud Director, when the SSL certificates are about to expire, the providers can renew or replace the certificates of the VMware Cloud Director Availability services and the certificates in the remaining disaster recovery infrastructure.

Replacing VMware Cloud Director Availability Certificates

Each VMware Cloud Director 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 VMware Cloud Director Availability service, configure VMware Cloud Director Availability to trust the certificate.

In a typical cloud deployment, the VMware Cloud Director Availability solution comprises of three types of appliances that operate the following VMware Cloud Director Availability services:

- Cloud Director Replication Management Appliance operating the Cloud Service and the Manager Service.
- Replicator Appliance operating the Replicator Service.
- Tunnel Appliance operating the Tunnel Service.

The Tunnel Service effectively proxies the tenants communication with the Cloud Service. When connecting through the remote Tunnel Service, the On-Premises to Cloud Director Replication Appliance sees only the certificate of the remote Cloud Service and the tenants do not see the certificates of the remote Replicator Service nor the certificate of the remote Tunnel Service.

Using a CA-Signed Certificate

Each VMware Cloud Director 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 for the Cloud Service, while the other services can continue to use self-signed certificates:

- Use a CA-signed certificate only for the Cloud Service. On the same Cloud Director Replication Management Appliance, you must use a self-signed certificate for the Replicator Service.
- Use self-signed certificates for the Tunnel Service and the Replicator Service. 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 Cloud Service. To keep the certificates unique, you must use self-signed certificates for the remaining VMware Cloud Director Availability services. Do not use the same wildcard certificate for more than one cloud site.

Managing the VMware Cloud Director Availability Certificates

Certificates are part of the communication chain used to validate the hosts and are also used for the VMware Cloud Director 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 Cloud Director Availability™ service.

Regenerate a Self-Signed Certificate

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

Procedure

1 Log in to the VMware Cloud Director 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 under **Configuration**, click **Settings**.
3 Under **Appliance settings**, next to **Certificate** click **Regenerate**.
4 In the **Regenerate Certificate** window, click **Apply**.

Results

After the certificate is regenerated, all VMware Cloud Director 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 **`cloud`**, **`manager`**, **`replicator`**, or **`tunnel`**.

Upload a CA-Signed Certificate

To prevent the Web browser from showing a certificate prompt every time a user opens the VMware Cloud Director 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 Cloud Service. Do not use the same certificate for any other VMware Cloud Director Availability service. For more information about wildcard certificates, see Replacing VMware Cloud Director Availability Certificates.

Procedure

1 Log in to the VMware Cloud Director 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 under **Configuration**, click **Settings**.
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 VMware Cloud Director 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 **`cloud`**, **`manager`**, **`replicator`**, or **`tunnel`**.

Replace the Cloud Service Certificate

Regenerate the Cloud Service self-signed SSL certificate or import a CA-signed certificate. After updating the certificate, re-establish the trust by re-pairing all cloud sites.

In VMware Cloud Director Availability 4.3 and later, replacing the Cloud Service certificate invalidates the trust only with the paired cloud sites. Replacing with a CA-signed certificate does not invalidate the trust with the paired on-premises sites and no longer requires re-pairing with on-premises sites.

To re-establish the trust with the cloud sites after replacing the certificate of the Cloud Service, re-pair with them.

Procedure

1 Log in to the management interface of the Cloud Director 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 SSL certificate of the Cloud Service.

   a In the left pane under **Configuration**, click **Settings**.

   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 To update the Cloud Service certificate, click **Apply**.

   You are logged out and the services automatically restart in a few minutes. After importing a CA-signed certificate, the Cloud Service creates a copy of the old certificate at `/opt/vmware/h4/cloud/config/keystore.p12.bak`.

3 In each paired cloud site, trust this new Cloud Service certificate.

   a In the left pane, click **Peer Sites**.

   b Select a cloud site and click **Repair**.

   c In the **Update Pairing** window, click **Update**.

   d To complete the trust re-establishment, accept the remote Cloud Service SSL certificate.

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

What to do next

When not using a CA-signed certificate for the Cloud Service, re-pair the paired on-premises sites with this cloud site. For more information, see Repair a Site.

Replace the Manager Service Certificate

Regenerate the Manager Service self-signed SSL certificate or import one. After updating this service certificate, repair the trust with the local Replicator Service instances and repair with all cloud sites.

In VMware Cloud Director Availability, replacing the Manager Service certificate:

- Invalidates the trust only:
  - with the paired cloud sites,
  - and with the Replicator Service instances in the local cloud site.
- On-premises sites that are paired automatically reestablish the trust after synchronizing or within 30 minutes. Re-pairing with on-premises sites is not necessary when replacing the SSL certificate of the Manager Service.

Post-certificate replacement

To re-establish the trust after replacing the certificate of the Manager Service, re-pair the registration of the Replicator Service instances in the local cloud site and re-pair with the cloud sites.

Procedure

1 Log in to the Manager Service 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 SSL certificate of the Manager Service.
   a In the left pane under **Configuration**, click **Settings**.
   b Under **Appliance settings** next to **Certificate**, select the certificate replacement method.

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

   c To update the Manager Service certificate, click **Apply**.

   You are logged out and the services automatically restart in a few minutes. After importing a certificate, the Manager Service creates a copy of the old certificate at `/opt/vmware/h4/manager/config/keystore.p12.bak`.

   After applying the new certificate, all Replicator Service instances and on-premises appliances become offline. Repair all Replicator Service instances in the cloud site. The on-premises appliances restore operations automatically within 30 minutes without additional actions.

   - Until the connectivity automatically restores, the tenants see the **Service connectivity** to the Manager Service as offline and all their replications are temporary in red health.
   - After re-pairing with all the Replicator Service instances and their connectivity restores, the replications return back to green health.

   Tenants do not have to perform additional actions with their on-premises appliances when the provider changes the Manager Service certificate as it only causes a temporary impact on the active replications.
3 Log in to the Manager Service 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 Manager Service certificate with the remaining Replicator Service instances in the local cloud site.

   a In the left pane, click **Replicator Services**.

   b In the **Replicator Services administration** page, select each local Replicator Service instance and click **Repair**.

   c In the **Details for replicator** window, enter the **root** user password of the Cloud Director Replication Management Appliance, the single sign-on credentials and click **Apply**.

   d To complete the trust re-establishment, verify the thumbprint and accept the SSL certificate of this local Replicator Service instance.

   Note Repeat this step and trust the new certificate of the Manager Service by selecting the remaining Replicator Service instances.

5 Log in to the management interface of the Cloud Director 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 In each paired cloud site, trust this new Manager Service certificate.

   a In the left pane, click **Peer Sites**.

   b Select a cloud site and click **Repair**.

   c In the **Update Pairing** window, click **Update**.

   d To complete the trust re-establishment, accept the remote Cloud Service SSL certificate.

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

Replace the Replicator Service Certificate

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

Replacing the SSL certificate of the Replicator Service unregisters it from the Manager Service in the local and in the remote sites. To repair the registration of the Replicator Service to the Manager Service in the remote site, you must re-establish the trust between the cloud sites. For more information, see Re-pair cloud sites backed by VMware Cloud Director.

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 Replicator Service service management interface for your deployment type.

Deployment type	Service Management Interface
Cloud Director Combined Appliance	**https://*Appliance-IP-Address*:8440/ui/admin**
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 Replicator Service instances to the Manager Service service on the local site.

   a Log in again to the Manager Service service management interface at **https://*Replication-Manager-IP-address*:8441/ui/admin**.

   On the **System Monitoring** tab all Replicator Service instances are `Offline`.

   b On the **Replicators** tab, select a Replicator Service instance and click **Repair**.

   c Enter the details of the Replicator Service instance and click **Apply**.

Option	Description
Appliance Password	The **root** user password for the Replicator Service appliance.
SSO User Name	A user name that has administrative privileges for the local site single sign-on domain, for example *Administrator@VSPHERE.LOCAL*.
SSO Password	The password for the administrative user.

   d Accept the SSL certificate of the Replicator Service service.

   e Repeat steps b to d for all Replicator Service instances that are registered to the Manager Service service in the local site.

   f After you repair the registrations for all Replicator Service instances, verify that no connectivity errors are reported on the **System Monitoring** tab.

5 In the service management interface of the Cloud Service 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 Tunnel Service Certificate

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

Replace the certificate of the Tunnel Service 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 Tunnel Service service management interface for your deployment type.

Deployment type	Service Management Interface
Cloud Director Combined Appliance	`https://Appliance-IP-Address:8442/ui/admin`
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**.

2 Log in as **root**.

3 Generate or upload a new certificate.

4 Log in to the management interface of the Cloud Director 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 under **Configuration**, click **Settings**.

6 Under **Service Endpoints** next to **Tunnel Service address**, click **Edit**.

7 In the **Tunnel Service Settings** window, click **Apply**.

8 Verify the thumbprint and accept the new Tunnel Service SSL certificate.

Results

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

instance connectivity. Without further actions, within 30 minutes VMware Cloud Director 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 VMware Cloud Director endpoint or its certificate, you must configure the VMware Cloud Director Availability services to work with the new certificate.

Configure to Accept a Renewed VMware Cloud Director Endpoint or Certificate

After changing the VMware Cloud Director endpoint or renewing its SSL certificate, configure VMware Cloud Director Availability to re-establish the trust with new certificate and communicate with VMware Cloud Director.

To re-establish the trust with VMware Cloud Director, in VMware Cloud Director Availability re-apply the endpoint with its address.

Prerequisites

Verify that the SSL certificate of VMware Cloud Director is successfully renewed. For information about generating and importing SSL certificates in VMware Cloud Director, see VMware KB 1026309.

Procedure

1 Log in to the VMware Cloud Director 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 under **Configuration**, click **Settings**.
3 To re-establish the trust, re-apply the address of the VMware Cloud Director endpoint.
   a Under **Service endpoints**, next to the VMware Cloud Director address click **Edit**.
   b Verify the URL of the VMware Cloud Director endpoint and click **Apply**.
   c Verify the thumbprint of the VMware Cloud Director certificate and click **Accept**.

Results

VMware Cloud Director Availability re-establishes the trust with VMware Cloud Director.

Configure VMware Cloud Director Availability to Accept the vCenter Server Lookup service Certificate

To enable single-sign on user authentication to the VMware Cloud Director Availability services, or after replacing the vCenter Server Lookup service certificate that is used as a replication or a

migration source or destination, configure the VMware Cloud Director Availability services to trust the updated certificate.

- By default, only the Replicator Service instances allow singe sign-on user authentication. To allow single sign-on for the remaining services, configure them with the address of vCenter Server Lookup service.
- After replacing the SSL certificate of the vCenter Server Lookup service, you must update all VMware Cloud Director Availability services configured with vCenter Server Lookup service to trust the updated certificate.

Prerequisites

- Verify that the SSL certificate is successfully renewed, and that the vCenter Server Lookup service is updated to use the renewed certificate.
- Verify that all infrastructure 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 Replicator Service instance to work with the renewed vCenter Server Lookup service certificate.

   Repeat this step for all Replicator Service instances.

   a In a Web browser, go to the Replicator Service management interface at **`https://`*`Replicator-Appliance-IP-address`*`/ui/admin`**.

   b Log in as the **root** user.

   c In the left pane, click **Settings**.

   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 vCenter Server Lookup service certificate appear.

   f Verify the thumbprint and accept the renewed vCenter Server Lookup service certificate.

   g In the left pane, click **System Health**.

   h To complete the Replicator Service configuration, click **Restart service**.

2 (Optional) If you are using a single sign-on login to the Cloud Service, configure it to work with the renewed vCenter Server Lookup service certificate.

   a In a Web browser, go to the Cloud Service management interface at **`https://`*`Cloud-Replication-Management-IP-address`*`/ui/admin`**.

   b Log in as the **root** user.

   c In the left pane under **Configuration**, click **Settings**.

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 vCenter Server Lookup service certificate appear.

f Verify the thumbprint and accept the renewed vCenter Server Lookup service certificate.

g In the left pane, click **System Health**.

h To complete the Cloud Service configuration, click **Restart service**.

3 (Optional) If you are using a single sign-on login to the Manager Service, configure it to work with the renewed vCenter Server Lookup service certificate.

a In a Web browser, go to the Manager Service service management interface at **`https://`*`Cloud-Replication-Management-IP-address`*`:8441/ui/admin`**.

b Log in as the **root** user.

c In the left pane, click **Settings**.

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 vCenter Server Lookup service certificate appear.

f Verify the thumbprint and accept the renewed vCenter Server Lookup service certificate.

g In the left pane, click **System Health**.

h To complete the Manager Service configuration, click **Restart service**.

4 (Optional) If you are using a single sign-on login to the Tunnel Appliance, configure the Tunnel Service to work with the renewed vCenter Server Lookup service certificate.

a In a Web browser, go to the Tunnel Appliance management interface at **`https://`*`Tunnel-Appliance-IP-address`*`/ui/admin`**.

b Log in as the **root** user.

c In the left pane, click **Settings**.

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 vCenter Server Lookup service certificate appear.

f Verify the thumbprint and accept the renewed vCenter Server Lookup service certificate.

g In the left pane, click **System Health**.

h To complete the Tunnel Service configuration, click **Restart service**.

Network Settings Configuration

After completing a VMware Cloud Director Availability appliance deployment, as a **system administrator** you can modify the network settings of the appliance by using the management interface.

Host Name Configuration

During the OVF deployment, as a **system administrator**, you can manually provide the appliance host name. If you skip this step, the DHCP server provides the host name. Some DHCP servers are not configured to provide a host name or do not support host name provisioning. In such cases, the appliance attempts to find the host name and performs a reverse DNS lookup by using the first non-link-local IP address of the default ens160 Ethernet adapter. If the request is successful, the appliance uses the provided domain name as a host name and ignores future host names received over DHCP. If the request is not successful, the appliance uses *photon-machine* as a host name.

After the deployment completes, you can modify the host name of the appliance by using the appliance management interface. Configuring a new host name overwrites the host name that is provided by DHCP.

DNS Settings Configuration

As a **system administrator**, you can configure the provisioning of DNS servers and Domain Search Path in manual or automatic mode.

Manual

As a **system administrator**, you must provide the static DNS settings.

Automatic

The DHCP server or Stateless Address Autoconfiguration (SLAAC) provides the DNS settings.

During the OVF deployment, you can manually provide the DNS settings. If you skip this step, the appliance uses the DNS settings provided by the DHCP server.

After the deployment completes, you can modify the DNS settings of the appliance by using the appliance management interface. When you provide the static DNS settings manually, all network adapters are configured to ignore the DNS settings that are provided by DHCP or SLAAC. Alternatively, you can switch to automatic mode by configuring one or more network adapters to use DHCP or SLAAC. Switching from manual to automatic mode overwrites all static DNS settings.

Network Adapter Configuration

During the OVF deployment, as a **system administrator**, you can provide the network adapter settings. If you do not populate the IP address, the adapter uses DHCPv4. After the deployment completes, you can change the adapter settings provided during deployment.

You can configure the network adapters in VMware Cloud Director Availability to use either IPv4 or IPv6 modes. You can provide the adapter settings manually or alternatively the settings can be received by using one of the following automatic mechanisms.

Manual

The manual adapter configuration requires you to provide a valid Classless Inter-Domain Routing (CIDR) static address. Enter the CIDR address as an IP address, followed by a forward slash and a network mask or a prefix length. You can also set a default gateway, that must be in the same network as the provided IP address. If a second adapter is configured manually with the same IP mode, skip setting the default gateway. You can also configure the maximum transmission unit (MTU), and if omitted, the appliance uses an MTU of 1500 bytes. You can set the static address, gateway, and MTU adapter settings for both IPv4 and IPv6 modes.

Automatic

DHCPv4, DHCPv6, or SLAAC can provide the automatic adapter configuration, depending on the IP mode.

By using DHCPv4 or DHCPv6, the network adapter is configured to:

- Use the DNS servers that are provided by the DHCP server.
- Use the search domains that are provided by the DHCP server.
- Ignore all routes that are provided by the DHCPv4 server, if the appliance has a default gateway configured.
- Remove all manually configured DNS settings such as DNS servers and search domains.
- Remove custom MTU settings.

By using SLAACv6, the network adapter is configured to:

- Enable IPv6 link-local addressing.
- Accept IPv6 Router Advertisement (RA).
- Accept DNS servers and search domains through RA.
- Remove all manually configured DNS settings such as DNS servers and search domains.
- Remove custom MTU settings.

Additional notes for the network adapter configuration:

- If there are multiple sources of DNS settings, for example two NICs that use two different DHCP servers, the DNS requests are sent to all DHCP servers. The appliance uses the first one that responds. To avoid potential issues, you must ensure that there are no conflicting settings. As a best practice, avoid such a configuration.

- To remove the configuration of the network adapter, you must click **Unconfigure** next to the IP mode. This action turns off the adapter and deletes all its settings, including static routes. Later, you can configure the adapter again, which turns it back on. Use this cleanup procedure, in case there are configuration leftovers that are causing unexpected network behavior.
- To change the manually configured default gateway, you must first remove the configuration of the network adapter that is configured with it.
- The upgrade to VMware Cloud Director Availability 4.0 attempts to migrate the network configuration of the old eth0 adapter. If using both IP modes before the upgrade, after the upgrade only one of them is enabled. Also, the upgrade replaces the eth0 adapter with the ens160 adapter.
- The appliance MTU size must match and must not exceed the MTU allowed in the network infrastructure environment.

Static Routes Configuration

VMware Cloud Director Availability 4.0 allows you as a **system administrator** to configure static routes that control how the network packets are sent to the destination.

In a typical environment, there is a default gateway that dynamically routes all the traffic to and from the external networks. Sometimes, you might want to route the traffic through another gateway. For example, you can use static routes when there is no dynamic route to the destination IP address, or when you want to override the dynamically learned route. To address such network setup, you can configure one or more static routes.

Note Applying any network changes can lead to temporary network outages. For example, the browser connectivity to the management interface is interrupted when being accessed through the network adapter that was just reconfigured.

Configure the Appliance Network Settings

As a **system administrator**, you can modify the host name, the DNS servers, and the Domain Search Path by using the management interface of the VMware Cloud Director Availability appliance.

Prerequisites

Verify that VMware Cloud Director Availability 4.0 or later is successfully deployed.

Procedure

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
   a. In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
   b. Select **Appliance login** and enter the **root** user password.
   c. Click **Login**.

2 In the left pane under **Configuration**, click **Settings**.

3 Under **Appliance settings** next to **Network**, click **Edit**.

4 In the **Network Settings** window, configure the network settings and click **Apply**.

   a Enter the appliance host name.

   b Enter the static DNS servers as a comma-separated list of DNS server addresses.

   c Enter the static Domain Search Path as a comma-separated list of search domains.

   Manually configuring the network settings overwrites the configuration provided by DHCP or by SLAAC.

Results

The VMware Cloud Director Availability appliance now uses the network settings that you configured.

What to do next

- You can configure the network adapters. For more information, see Configure a Network Adapter.
- You can use the local domain as a top-level domain in VMware Cloud Director Availability appliances. For more information, see VMware KB 79088.

Configure a Network Adapter

As a **system administrator**, you can modify the network adapter settings, such as IP Mode and type, address, gateway, and MTU by using the management interface of the VMware Cloud Director Availability appliance.

Note Applying any network changes can lead to temporary network outages. For example, the browser connectivity to the management interface is interrupted when being accessed through the network adapter that was just reconfigured.

Prerequisites

Verify that VMware Cloud Director Availability 4.0 or later is successfully deployed.

Procedure

1 Log in to the management interface of the VMware Cloud Director Availability appliance.

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

   b Under **Appliance login**, enter the **root** user password.

   c Click **Login**.

2 In the left pane under **Configuration**, click **Settings**.

3 Under **Appliance settings**, expand the **Network** section.

You can see all the network adapters that are added to the appliance.

4 Next to the adapter name click **Edit**.

5 In the **Settings** window, configure the network settings and click **Apply**.

a To select an IP mode, click **IPv4**, **IPv6**, or **Unconfigured**.

By selecting **Unconfigured**, you turn off the adapter and delete all its settings, including static routes. Use this cleanup procedure, in case there are configuration leftovers that are causing unexpected network behavior.

b Click **Type** and select how to provide the network configuration.

Option	Description
DHCP	If you select DHCP to provide the network configuration, all manually configured network settings, such as DNS servers, search domains, static routes, and MTU size are removed.
SLAAC	If you select SLAAC to provide the network configuration, all manually configured network settings, such as DNS servers, search domains, static routes, and MTU size are removed.
Static	Enter the static configuration. 1 In the **Address/Prefix** text box, enter a CIDR address - IP address, followed by a forward slash and a network mask or a prefix length. 2 In the **Gateway** text box, enter a gateway that is in the same network as the provided IP address. For each IP mode, you can use only one default gateway. If you are configuring a second adapter in the same IP mode, you must not enter a default gateway. 3 In the **MTU (bytes)** text box, enter the maximum transmission unit size in bytes. The default is 1500 bytes.

The selected network adapter of the VMware Cloud Director Availability appliance is configured with the provided settings.

What to do next

- You can configure the DNS, the appliance host name, and the Domain Search Path. For more information, see Configure the Appliance Network Settings.
- You can add additional network adapters to configure. For more information, see Add an Additional Network Adapter.
- You can use the local domain as a top-level domain in VMware Cloud Director Availability appliances. For more information, see VMware KB 79088.

Configure Static Routes

To route the network packets through a specific gateway, as a **system administrator** you can configure static routes by using the management interface of the VMware Cloud Director Availability appliance.

Note Applying any network changes can lead to temporary network outages. For example, the browser connectivity to the management interface is interrupted when being accessed through the network adapter that was just reconfigured.

Prerequisites

Verify that VMware Cloud Director Availability 4.0 or later is successfully deployed.

Procedure

1. Log in to the management interface of the VMware Cloud Director Availability appliance.
   a. In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
   b. Select **Appliance login** and enter the **root** user password.
   c. Click **Login**.
2. In the left pane under **Configuration**, click **Settings**.
3. Under **Appliance settings**, expand the **Network** section.

   You can see all the network adapters that are added to the appliance.
4. To configure the static routes for a network adapter, next to the adapter name click **Static routes**.

   The static routes are persistent for the selected IP mode of the adapter. If you change the IP mode, all static routes are deleted.

5 In the **Static routes** window, configure the static routes for the selected network adapter.

The routes that the management interface shows do not contain the whole routing table. The management interface only shows the manually configured routes.

a To add a new static route, enter the following route details and click **Add**.

Option	Description
Destination	You must enter the specific IP address or the whole subnet of the target network.
Gateway	You must enter the IP address of the specific gateway that knows how to route the traffic.
Metric	You can enter a lower value to prioritize the route or a higher value to deprioritize the route. As a best practice, avoid the route prioritization and use the default value of 0.

b To remove a static route, click **Delete**.

To edit a static route entry, you must delete it and add it again.

c To apply the network changes, click **Apply**.

Results

The selected network adapter of the VMware Cloud Director Availability appliance is configured with the provided static routes.

What to do next

You can add additional network adapters to add routes to. For more information, see Add an Additional Network Adapter.

Add an Additional Network Adapter

As a **system administrator**, you can configure additional network adapters by using the vSphere Client. The newly added adapters can be later configured by using the management interface of the VMware Cloud Director Availability appliance.

Prerequisites

Verify that the VMware Cloud Director Availability 4.0 or later appliance is successfully deployed.

Procedure

1 Log in to the vCenter Server instance by using the vSphere Client.

2 Navigate to the VMware Cloud Director Availability virtual machine.

3 Right-click the VMware Cloud Director Availability virtual machine and from the drop-down menu select **Edit Settings**.

4 In the **Edit Settings** window, click **Add new device > Network Adapter**.

5 Select the appropriate network.

6 Select **VMXNET 3** as the adapter type and **Automatic** for the MAC address.

7 Verify that **Connected** is selected and click **OK**.

The VMware Cloud Director Availability virtual machine is configured with the new adapter.

8 Log in to the management interface of the VMware Cloud Director Availability appliance.

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

Use the IP address of the previously existing network adapter.

b Select **Appliance login** and enter the **root** user password.

c Click **Login**.

9 In the left pane, click **Settings**.

10 Under **Appliance settings**, expand the **Network** section.

You can see all the network adapters that are added to the appliance. The newly added adapter is listed as **Unconfigured**.

What to do next

You can configure the new network adapter. For more information, see Configure a Network Adapter.

Select the Endpoint Address for each Network Adapter

Control which network interface the appliance uses for specific communication traffic by selecting the endpoint address. In the Tunnel Appliance, select the address for communication with the local cloud appliances. In each Replicator Appliance instance, select the addresses for management traffic, and for incoming and for outgoing replication traffic.

Selecting the endpoint addresses controls the type of traffic the cloud appliances expect on which network interface cards (NICs). The traffic control allows for more specific network topologies and is not intended for traffic isolation between the data and the management network traffic.

Note

- Selecting endpoint address associates it with the IP address. To apply a new endpoint address after the selected IP address changes, manually select the updated IP address for the endpoint re-association.
- The selected IP address for each endpoint must be configured with a static IP address.

Tunnel Appliance

In the management interface of the Tunnel Appliance, to control the internal traffic in the site you can select an endpoint address for the communication from the Replicator Appliance instances and from the Cloud Director Replication Management Appliance to the Tunnel Appliance, avoiding their communication over the external-facing Tunnel Appliance address. Controlling the Tunnel Appliance traffic avoids routing the traffic from the local cloud appliances through the Internet-facing NIC of the Tunnel Appliance.

Replicator Appliance instances

In the management interface of each Replicator Appliance instance, to control the traffic you can select the following endpoint addresses.

- For management traffic, between the local cloud appliances in the site.
- For outgoing replication data traffic, to the destination ESXi hosts.
- For incoming replication data traffic, from the source ESXi hosts.

When the Replicator Appliance instances are on a separate network from the ESXi hosts or the Tunnel Appliance, selecting these endpoints directly routes the heavy replication data traffic avoiding the router and reducing the impact over the entire internal infrastructure network.

Prerequisites

Verify that VMware Cloud Director Availability 4.3 or later is deployed in the cloud site.

Procedure

1 Select the Tunnel Appliance endpoint address for controlling the traffic from the local cloud appliances.

   a In a Web browser, go to `https://Tunnel-Appliance-IP-Address`.

   The `https://Tunnel-Appliance-IP-Address/ui/admin` login page opens.

   b Enter the password of the **root** user and click **Login**.

   The **Settings** page opens.

   c Under **Appliance settings**, click **Edit** next to the **Traffic Control** section.

   The **Traffic Control** window opens.

   d From the **Tunnel Address** drop-down menu, select the endpoint IP address for the communication from the local cloud appliances and click **Apply**.

2 Select the Replicator Appliance instance endpoint addresses for controlling the management traffic and the traffic from the local ESXi hosts.

   a In a Web browser go to `https://Replicator-Appliance-IP-Address`.

   The `https://Replicator-Appliance-IP-Address/ui/admin` login page opens.

   b Enter the password of the **root** user and click **Login**.

   The **System Health** page opens.

c In the left pane, click **Settings**.

d Under **Appliance settings** click **Edit** next to the **Traffic Control** section.

The **Traffic Control** window opens.

e From the **Management Address** drop-down menu, select the endpoint IP address for the management traffic between the local cloud appliances, where the Tunnel Appliance redirects all traffic when not setting a specific data endpoint.

f From the **NFC Address** drop-down menu select the endpoint IP address for the outgoing Network File Copy (NFC) traffic to the destination ESXi host. All outgoing data traffic to the ESXi hosts goes through this endpoint address.

g From the **LWD Address** drop-down menu select the endpoint IP address for the incoming Lightweight Delta Protocol (LWD) traffic. This endpoint address receives the incoming data traffic from the local source ESXi host.

h To confirm the selected endpoint addresses, click **Apply**.

Repeat this step for the remaining Replicator Appliance instances in the cloud site.

3 After configuring all Replicator Appliance instances, in the Cloud Director Replication Management Appliance enable tunneling to the new Tunnel Appliance endpoint address.

a In a Web browser, go to `https://Cloud-Replication-Management-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 under the **Configuration** section, click **Settings**.

e Under **Service endpoints**, next to **Tunnel Service address** click **Edit**.

f In the **Tunnel Service Settings** window, enter the **root** user password of the Tunnel Appliance.

The **Tunnel Service Endpoint address** is already populated and the **Appliance user** is set to **root**.

g Click **Apply**.

h Verify the thumbprint and accept the certificate of the Tunnel Service.

Results

The selected endpoint addresses control the incoming and outgoing traffic.

What to do next

You can ensure that the selected endpoint addresses do not affect the VMware Cloud Director Availability connectivity. For more information, see Verify the Uptime and the Local and the Remote Connectivity in the Cloud.

Command-Line Network Configuration

If the management interface is not available, as a **system administrator**, you can configure all network settings by using the command-line interface of the VMware Cloud Director Availability appliance.

Caution Only use the following `net.py` commands in case you cannot access the management interface. You must not use any other command-line network configuration, for example: the `ip` command, VAMI scripts, must not manually modify configuration files, and other network settings. Do not automate or use in scripts the `net.py` commands.

You can run the following `net.py` commands in any order.

Prerequisites

- Verify that the VMware Cloud Director Availability 4.0 or later appliance is successfully deployed.
- Verify that before running any of the following commands, you understand the general network configuration in VMware Cloud Director Availability. For more information, see Network Settings Configuration.

Procedure

1. Connect to the VMware Cloud Director Availability by using a Secure Shell (SSH) client.
   a. Open an SSH connection to *Appliance-IP-Address*.
   b. Log in as the **root** user.
2. To retrieve all available network adapters, run: `/opt/vmware/h4/bin/net.py nics-status`.

```
$ /opt/vmware/h4/bin/net.py nics-status
[
    {
        "addresses": [
            "fe80::250:56ff:fea9:7c8c/64"
        ],
        "configMode": "SLAAC_V6",
        "gateway": null,
        "mac": "00:50:56:a9:7c:8c",
        "mtu": 1500,
        "name": "ens192",
        "state": "degraded (configured)"
    },
    {
        "addresses": [
            "10.71.218.128/21"
        ],
        "configMode": "DHCP_V4",
        "gateway": "10.71.223.253",
        "mac": "00:50:56:a9:0e:65",
        "mtu": 1500,
```

```
        "name": "ens160",
        "state": "routable (configured)"
    }
]
```

3 To retrieve the status of a specific network adapter, run: `/opt/vmware/h4/bin/net.py nic-status <adapter-name>`.

```
$ /opt/vmware/h4/bin/net.py nic-status ens160
{
    "addresses": [
        "10.71.218.128/21"
    ],
    "configMode": "DHCP_V4",
    "gateway": "10.71.223.253",
    "mac": "00:50:56:a9:0e:65",
    "mtu": 1500,
    "name": "ens160",
    "state": "routable (configured)"
}
```

4 To turn off a specific network adapter and delete all its settings, including static routes, run: `/opt/vmware/h4/bin/net.py unconfigure-nic <adapter-name>`.

```
$ /opt/vmware/h4/bin/net.py unconfigure-nic ens192
{
    "addresses": [],
    "configMode": "UNCONFIGURED",
    "gateway": null,
    "mac": "00:50:56:a9:7c:8c",
    "mtu": 1500,
    "name": "ens192",
    "state": "off (unmanaged)"
}
```

5 To configure a specific network adapter to use DHCPv4, run: `/opt/vmware/h4/bin/net.py configure-nic <adapter-name> --dhcp4`.

The command configures the network adapter and exits instantly, although in the background the network settings are received and handled asynchronously.

```
$ /opt/vmware/h4/bin/net.py configure-nic ens192 --dhcp4
{
    "addresses": [],
    "configMode": "DHCP_V4",
    "gateway": null,
    "mac": "00:50:56:a9:7c:8c",
    "mtu": 1500,
    "name": "ens192",
    "state": "carrier (configuring)"
}
```

6 To configure a specific network adapter to use DHCPv6, run: `/opt/vmware/h4/bin/net.py configure-nic <adapter-name> --dhcp6`.

The command configures the network adapter and exits instantly, although in the background the network settings are received and handled asynchronously.

```
$ /opt/vmware/h4/bin/net.py configure-nic ens192 --dhcp6
{
    "addresses": [],
    "configMode": "DHCP_V6",
    "gateway": null,
    "mac": "00:50:56:a9:7c:8c",
    "mtu": 1500,
    "name": "ens192",
    "state": "no-carrier (configuring)"
}
```

7 To configure a specific network adapter to use SLAAC, run: `/opt/vmware/h4/bin/net.py configure-nic <adapter-name> --slaac`.

The command configures the network adapter and exits instantly, although in the background the network settings are received and handled asynchronously.

```
$ /opt/vmware/h4/bin/net.py configure-nic ens192 --slaac
{
    "addresses": [],
    "configMode": "SLAAC_V6",
    "gateway": null,
    "mac": "00:50:56:a9:7c:8c",
    "mtu": 1500,
    "name": "ens192",
    "state": "no-carrier (configuring)"
}
```

8 To configure a specific network adapter to use a static IP, run: `/opt/vmware/h4/bin/net.py configure-nic <adapter-name> --static --address <CIDR> --gateway <IP> --mtu <MTU-bytes>`.

```
$ /opt/vmware/h4/bin/net.py configure-nic ens192 --static --address 172.16.0.2/18 --gateway
172.16.0.1 --mtu 1400
{
    "addresses": [
        "172.16.0.2/18"
    ],
    "configMode": "DHCP_V4",
    "gateway": "172.16.0.1",
    "mac": "00:50:56:a9:0e:65",
    "mtu": 1400,
    "name": "ens192",
    "state": "routable (configured)"
}
```

9 To see the manually configured static routes list for a specific network adapter, run: `/opt/vmware/h4/bin/net.py list-routes <adapter-name>`.

```
$ /opt/vmware/h4/bin/net.py list-routes
ens192
[
    {
        "destination": "1.2.3.4",
        "gateway": "5.6.7.8",
        "metric": 0
    },
    {
        "destination": "10.0.0.0/16",
        "gateway": "9.9.9.9",
        "metric": 0
    },
    {
        "destination": "40.40.40.40",
        "gateway": "50.50.50.50",
        "metric": 0
    }
]
```

10 To add a static route to a specific network adapter, run: `/opt/vmware/h4/bin/net.py add-route <adapter-name> <destination IP or subnet CIDR> <gateway> <optional-metric>`.

```
$ /opt/vmware/h4/bin/net.py add-route ens160 99.99.99.99 10.0.0.42
[
    {
        "destination": "99.99.99.99",
        "gateway": "10.0.0.42",
        "metric": 0
    }
]
```

11 To remove a static route from a specific network adapter, run: `/opt/vmware/h4/bin/net.py remove-route <adapter-name> <destination IP or subnet CIDR> <gateway> <metric>`.

Ensure that the destination IP, gateway, and metric exactly match the rule to delete.

```
$ /opt/vmware/h4/bin/net.py remove-route ens160 99.99.99.99 10.0.0.42
[]
```

Stretching On-Premises Layer 2 Networks in the Cloud

During on-premises to the cloud migrations, to allow network connectivity between already migrated and not yet migrated virtual machines as in the same network segment, stretch the on-premises networks across the cloud site. Layer 2 VPN (L2 VPN) stretches the L2 networks across the sites.

VMware Cloud Director Availability L2 Stretch

By using NSX and its L2 VPN service technology, VMware Cloud Director Availability stretches on-premises L2 networks across the cloud site.

Cloud Site

To establish the server L2 VPN session, VMware Cloud Director Availability 4.2 uses VMware NSX. In addition to NSX, VMware Cloud Director Availability 4.2.1 and later also support VMware NSX® Data Center for vSphere® for stretching the L2 network.

On-Premises Site

To establish the client L2 VPN session, in a site not managed by NSX download and deploy a standalone VMware® NSX Edge™ appliance, called NSX Autonomous Edge.

To provide self-service for the tenants, VMware Cloud Director Availability manages the entire L2 VPN configuration of the necessary NSX network infrastructure, both in the cloud site and in on-premises sites. As an alternative to using VMware Cloud Director Availability for the L2 stretch, the service provider can perform the entire L2 VPN configuration and management solely in NSX, with the added complexity.

L2 Stretch Use Case

While migrating workloads consisting of several virtual machines, some of the virtual machines can get migrated to the cloud site with the remaining virtual machines of the workload running on-premises. By stretching the network across the two data centers the communication between the migrated and the remaining virtual machines continues as if they operate across the same network segment. The virtual machines remain on the same subnet during the migration between the sites as the stretched network represents a single subnet with a single broadcast domain. When using NSX Autonomous Edge for the L2 stretch, the on-premises virtual machines can only run on VLAN-based networks of distributed switches, that is, distributed port groups.

For the cloud providers, the L2 VPN allows on-boarding tenants without modifying existing IP addresses used by their workloads and applications. Since the IP addresses of the virtual machines do not change upon migration, migrations of the tenants workloads between different network sites are seamless.

In addition to supporting data center migration, on-premises networks stretched with an L2 VPN are useful for disaster recovery plans and dynamically engaging off-premise compute resources and meeting the increased demand.

Internet Protocol Security (IPSec) Tunnel

When using NSX for an L2 stretch, a route-based IPSec tunnel between the server L2 VPN and the client L2 VPN secures the network traffic flowing between the two networks connected over a public network through IPSec gateways called endpoints.

- For information about IPSec VPN when using NSX, see Understanding IPSec VPN in the *VMware NSX* documentation.

- For information about IPSec VPN when using NSX Data Center for vSphere, see IPSec VPN Overview in the *VMware NSX Data Center for vSphere* documentation.

L2 VPN Tunnel

The L2 VPN tunnel carries only workload traffic and supports network address translation (NAT) through IPSec L2 VPN.

- For information about L2 VPN when using NSX, see Understanding Layer 2 VPN in the *VMware NSX* documentation.
- For information about L2 VPN when using NSX Data Center for vSphere, see L2 VPN Overview in the *VMware NSX Data Center for vSphere* documentation.

Multiple client L2 VPN sessions cannot pair to a single server L2 VPN session. An NSX Autonomous Edge can stretch networks from a single vSphere Distributed Switch (VDS), that is, the VDS of the trunk network. To stretch networks from more than one VDS, deploy multiple NSX Autonomous Edge instances.

On-premises, a single NSX Autonomous Edge instance can support a single client L2 VPN session, that can stretch multiple virtual machine networks. To stretch additional client L2 VPN sessions, deploy additional NSX Autonomous Edge instances.

In the cloud site, for information about the scale number of L2 stretched networks to a cloud site, see VMware Cloud Director Availability Configuration Limits.

Note Cannot establish the L2 VPN tunnel until both the server L2 VPN and the client L2 VPN are configured, and a stretched network is created by selecting client network for each server network. For the procedure steps order, see Stretching Layer 2 Networks On-Premises.

Create a Server L2 VPN Session with NSX in the Cloud

By using the management interface of VMware Cloud Director Availability in the cloud site backed by NSX, organization administrators create the server side of the L2 VPN session, enabling the L2 stretch of one or more networks across the on-premises site.

After preparing VMware Cloud Director with an external network and an edge gateway as per the two steps in the prerequisites, and the on-premises site as per the Stretching Layer 2 Networks On-Premises procedure, follow the procedure below and create the server L2 VPN session.

Prerequisites

- Verify that in both the cloud site and in the on-premises site VMware Cloud Director Availability 4.2 or later is successfully deployed.
- Verify that the on-premises site is prepared for an L2 VPN session with NSX Autonomous Edge. For information about the order of the steps of the procedure, see Stretching Layer 2 Networks On-Premises.

- Verify that NSX 3.1 or later is deployed in the cloud site to allow stretching of routed and isolated networks.

  Note
  - Using earlier NSX versions allows only routed networks stretch.
  - For NSX Data Center for vSphere (NSX-V), skip this procedure and see Create a Server L2 VPN Session with NSX Data Center for vSphere in the Cloud.

- Verify that VMware Cloud Director 10.1.0 or 10.2.1 is deployed to allow a single network stretch, or that VMware Cloud Director 10.2.2 or later is deployed to allow multiple networks stretches. The L2 stretch by using NSX does not support VMware Cloud Director versions earlier than 10.2.

  Note VMware Cloud Director 10.3.1 and later do not support isolated networks. To stretch isolated networks use VMware Cloud Director 10.3.0 or earlier.

- Verify that the **Organization Administrator** user has rights to View L2 VPN and Configure L2 VPN. For information about the rights, see Users and Sessions in the *Security Guide*.
- Verify that VMware Cloud Director is prepared to use NSX network resources, after adding an external network backed by a tier-0 gateway, then adding an NSX edge gateway that allows establishing the server L2 VPN session while providing the organization VDC networks with connectivity to external networks:

  a Verify that in VMware Cloud Director the NSX backed external network is added. For more information, see Add an External Network That Is Backed by an NSX Tier-0 Gateway in the *VMware Cloud Director* documentation.

  Note The VPN service is not supported in an active-active HA (high availability) mode of the tier-0 gateway. For more information, see Add a Tier-0 Gateway in the *NSX* documentation.

  b Verify that in VMware Cloud Director the NSX edge gateway is added. For more information, see Add an NSX Edge Gateway in the *VMware Cloud Director* documentation.

Procedure

1 Log in to the management interface of the Cloud Director 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, under the **Configuration** section click **L2 Stretch**.

3 Click **L2 VPN Sessions**.

4 From the **Gateway** menu, select the edge gateway and click **New**.

The **NSX Gateway** menu lists both NSX and NSX-V edge gateways that are registered and added in VMware Cloud Director. For information about using NSX-V for server L2 sessions, see Create a Server L2 VPN Session with NSX Data Center for vSphere in the Cloud.

5 In the **New L2 VPN server session** window, configure the server L2 VPN session and click **Create**.

a In the **Name** text box, enter a name for this server L2 VPN session.

b In the **Local Address** text box, enter an IP address residing in the IP pool of the edge gateway at the server side of the L2 VPN session.

The local IP address is a static IP address within the allocated IP range of the NSX edge gateway hosting the server L2 VPN session.

c In the **Remote Address** text box, enter the on-premises IP address at the client side of the L2 VPN session.

Usually the remote IP address is the static endpoint IP address of the NSX Autonomous Edge on-premises. For more information, see Configure the Networks of the NSX Autonomous Edge On-Premises.

Note Ensure that the network communication between the local IP address in the cloud and the remote IP address on-premises exists unobstructed.

d In the **Pre-shared Key** text box, enter the pre-shared key as provided by your network administrator.

Enter only visible ASCII characters, including space, excluding non-printable characters like Null, BEL, and so on. The pre-shared key must meet the following complexity requirements:

- At least 8 characters
- At least one uppercase letter
- At least one lowercase letter
- At least one digit
- At least one special character

e In the **Tunnel Interface** text box, enter a private, non-routable subnet address in a CIDR notation.

f Under **Server Network(s)**, to establish an L2 stretch select the server side networks to stretch.

The number of available server networks to select, depends on the version of VMware Cloud Director. For information about the VMware Cloud Director versions, see the prerequisites above.

Note Attempting to delete the server L2 VPN session takes several minutes. Do not attempt to recreate the server L2 VPN session immediately after deletion as it fails due to the deletion progress in the background.

Results

You created the server L2 VPN session in the cloud site.

What to do next

You can now create the client L2 VPN session that completes the L2 stretch. For more information, see Stretching Layer 2 Networks On-Premises.

Create a Server L2 VPN Session with NSX Data Center for vSphere in the Cloud

By using the management interface of VMware Cloud Director Availability in the cloud site backed by NSX Data Center for vSphere, the service provider registers the NSX Manager. Then the service provider or the organization administrator creates the server L2 VPN session enabling the L2 stretch of one or more networks across the on-premises site.

After preparing VMware Cloud Director with an external network and an edge gateway as per the two steps in the prerequisites, and the on-premises site as per the Stretching Layer 2 Networks On-Premises procedure, follow the procedure below and register the NSX Manager as a service provider. Then as either a service provider or an organization administrator, create the server side of the L2 VPN session.

Prerequisites

- Verify that in both the cloud site and in the on-premises site VMware Cloud Director Availability 4.2.1 or later is successfully deployed.
- Verify that the on-premises site is prepared for an L2 VPN session with NSX Autonomous Edge. For information about the order of the steps of the procedure, see Stretching Layer 2 Networks On-Premises.

- Verify that in the cloud site NSX Data Center for vSphere (NSX-V) 6.4.10 or later is deployed to allow stretching of routed networks after registering the NSX Manager.

  Note

  - NSX Data Center for vSphere stretches only **Routed** type networks only with interface type **Subinterface**, not **Internal** nor **Distributed**, and cannot stretch **Isolated** nor **Direct** type networks. NSX Data Center for vSphere can stretch only VXLAN and VLAN OrgVDC routed networks connected to the **Trunk** interface, and cannot stretch networks connected to the **Uplink** nor **Internal** interfaces. **Guest VLAN Allowed** must be deselected and if at some point it was selected, recreate the network for stretch from scratch.
  - For NSX, skip this procedure and see Create a Server L2 VPN Session with NSX in the Cloud.

- Verify that before stretching VLAN routed networks, in vSphere the service provider first created and associated the trunk interface with the edge gateway.
- Verify that VMware Cloud Director 10.0.0.3 or later is deployed in the cloud site.
- Verify that to register the NSX Manager with the Cloud Service for the first time, the service provider authenticates in VMware Cloud Director Availability as a **System Administrator** user.
- Verify that VMware Cloud Director is prepared to use vSphere backed network resources, after adding an external network, then adding an NSX Data Center for vSphere edge gateway that allows establishing the server L2 VPN session while providing the organization VDC networks with connectivity to external networks:

  a Verify that in VMware Cloud Director the vSphere backed external network is added. For more information, see Add an External Network That Is Backed by vSphere Resources in the *VMware Cloud Director* documentation.

  b Verify that in VMware Cloud Director the NSX Data Center for vSphere edge gateway is added. For more information, see Add an NSX Data Center for vSphere Edge Gateway in the *VMware Cloud Director* documentation.

Procedure

1 Log in to the management interface of the Cloud Director 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, under the **Configuration** section click **L2 Stretch**.

3 Click **NSX-V Managers** and select an NSX Manager with an `Unconfigured` status.

4 Click **Edit**.

5 In the **Configure** window, register the NSX Manager with the Cloud Service.

   a In the **Password** text box, enter the **admin** user password for the NSX Manager.

   b To register the NSX Manager for L2 stretch management by VMware Cloud Director Availability, click **Configure**.

      Verify the thumbprint and accept the SSL certificate of the NSX Manager.

   The NSX Manager is now registered, shows `Up` status, and is ready for creating the server L2 VPN session.

6 Click **L2 VPN Sessions**.

7 From the **NSX Gateway** menu, select the edge gateway and click **New**.

   The **NSX Gateway** menu lists both NSX-V and NSX edge gateways that are registered and added in VMware Cloud Director. For information about using NSX for server L2 sessions, see Create a Server L2 VPN Session with NSX in the Cloud.

8 In the **New L2 VPN server session** window, configure the server L2 VPN session and click **Create**.

   a In the **Name** text box, enter a name for this server L2 VPN session.

   b In the **Local Address** text box, enter an IP address residing in the IP pool of the edge gateway at the server side of the L2 VPN session.

      The local IP address is a static IP address within the allocated IP range of the NSX edge gateway hosting the server L2 VPN session.

   c In the **Remote Address** text box, enter the on-premises IP address at the client side of the L2 VPN session.

      Usually the remote IP address is the static endpoint IP address of the NSX Autonomous Edge on-premises. For more information, see Configure the Networks of the NSX Autonomous Edge On-Premises.

      Note Ensure that the network communication between the local IP address in the cloud and the remote IP address on-premises exists unobstructed.

d In the **Pre-shared Key** text box, enter the pre-shared key as provided by your network administrator.

   Enter only visible ASCII characters, including space, excluding non-printable characters like Null, BEL, and so on. The pre-shared key must meet the following complexity requirements:

   - At least 8 characters
   - At least one uppercase letter
   - At least one lowercase letter
   - At least one digit
   - At least one special character

e In the **Tunnel Interface** text box, enter a private, non-routable subnet address in a CIDR notation.

f Under **Server Network(s)**, to establish an L2 stretch select the server side networks to stretch.

   - The available networks for selection are filtered to show only OrgVDC networks connected to the trunk interface of the NSX Data Center for vSphere.
   - The number of available server networks for selection, depends on the version of VMware Cloud Director. For information about the VMware Cloud Director versions, see the prerequisites above.

Note

- Cannot change or edit the selected networks for stretching when using NSX Data Center for vSphere. To modify the stretched networks, click **Delete** and recreate the server L2 VPN session.
- Attempting to delete the server L2 VPN session takes several minutes. Do not attempt to recreate the server L2 VPN session immediately after deleting as it fails due to the deletion progress in the background.

Results

You created the server L2 VPN session in the cloud site.

What to do next

You can now create the client L2 VPN session that completes the L2 stretch. For more information, see Stretching Layer 2 Networks On-Premises.

Events and Notifications

You can monitor the events that VMware Cloud Director Availability generates either by using a syslog server, or in VMware Cloud Director, or by using email delivery for the notifications.

Event Notifications Delivery Channels

For VMware Cloud Director Availability monitoring in the cloud site, the Cloud Service delivers information about significant events by using the following delivery channels:

- **Syslog**

  As a **service provider**, you can use the syslog protocol to deliver the event notifications to a preconfigured syslog server, for example vRealize Log Insight. To enter the syslog server IP address and UDP port, see Configure Provider Events.

- **Cloud Director**

  This event notification delivery channel is available for both **service provider** and **tenant** users. In the VMware Cloud Director, as an **OrgAdmin** user, you can monitor VMware Cloud Director Availability events and also monitor events about user actions for replications owned by the same user. As a **SysAdmin** user, you can monitor all events, including the events that **OrgAdmin** users see, with additional event details.

- **Email**

  This event notification delivery channel is available for both **service provider** and **tenant** users. In VMware Cloud Director, as an **OrgAdmin** user, you can configure an SMTP server for the events notifications. VMware Cloud Director Availability uses the SMTP configuration of VMware Cloud Director and to receive email notifications from the Cloud Service, configuring the SMTP settings in VMware Cloud Director is required.

  - For information about configuring the email notifications as a **service provider**, see Configure the System Email Settings in the *VMware Cloud Director **Service Provider** Admin Portal Guide*.
  - For information about configuring the email notifications as a **tenant** user, see Modify Your Email Settings in the *VMware Cloud Director **Tenant** Portal Guide*.

All the delivery channels carry the same notification information, that is formatted according to the delivery method. To receive events notifications, you can use a single channel, all three channels, or not use any of the event notification channels.

- To configure the notifications and their delivery channels as a **service provider**, see Configure Provider Events.
- To configure the notifications and their delivery channels as a **tenant** user, see Forward Tenant Event Notifications in the *User Guide* document.

Event Types

Based on the generation mechanism, VMware Cloud Director Availability logs the following two types of events:

Management Events

User actions generate these events, for example, starting a replication, replication operations, policy changes, and others. For more information about the management event types, see the following table.

VMware Cloud Director Availability logs the following two types of management events:

System Management Events

Only available for **service provider** users.

Replication Management Events

Available for both **service provider** and **tenant** users.

Monitoring Events

The system generates these events, for example, periodic checks that are generated when a certain criteria is met. For more information about the monitoring event types, see the following table.

VMware Cloud Director Availability logs the following two types of monitoring events:

System Monitoring Events

Only available for **service provider** users.

Replication Monitoring Events

Available for both **service provider** and **tenant** users.

Table 2-4. Management Events

Event Type	Log Level	Resource ID	Description	Details
start	INFO	Replication ID	The replication of the *vm-name* virtual machine started.	If the replication is a migration, what is the replication direction: cloud to cloud, cloud to on-premises, or on-premises to cloud, and warning messages
start	ERROR	N/A	The replication of the *vm-name* virtual machine failed to start.	If the replication is a migration, what is the replication direction: cloud to cloud, cloud to on-premises, or on-premises to cloud, and a stack trace
stop	INFO	Replication ID	The replication of the *vm-name* virtual machine stopped.	Warning messages
sync	INFO	Replication ID	A replication instance is created for the replicated *vm-name* virtual machine.	The latest instance ID
sync	ERROR	Replication ID	Failed to create a replication instance for the replicated *vm-name* virtual machine.	A stack trace

Table 2-4. Management Events (continued)

Event Type	Log Level	Resource ID	Description	Details
failover	INFO	Replication ID	The replicated *vm-name* virtual machine failed over.	Recovery information and warning messages
failover	ERROR	Replication ID	The failover failed for the replicated *vm-name* virtual machine.	A stack trace
migrate	INFO	Replication ID	The replicated *vm-name* virtual machine is migrated.	Recovery information and warning messages
migrate	ERROR	Replication ID	The migration failed for the replicated *vm-name* virtual machine.	A stack trace
failoverTest	INFO	Replication ID	The test image is created for the replicated *vm-name* virtual machine.	Recovery information and warning messages
failoverTest	ERROR	Replication ID	The test image creation failed for the replicated *vm-name* virtual machine.	A stack trace
failoverTestCleanup	INFO	Replication ID	The cleanup of the test image is successful for the replicated *vm-name* virtual machine.	Warning messages
failoverTestCleanup	ERROR	Replication ID	The cleanup of the test image failed for the replicated *vm-name* virtual machine.	A stack trace
pause	INFO	Replication ID	The replication synchronization is paused for the replicated *vm-name* virtual machine.	N/A
pause	ERROR	Replication ID	Failed to pause the replication synchronization for the replicated *vm-name* virtual machine.	A stack trace
resume	INFO	Replication ID	The replication synchronization is resumed for the replicated *vm-name* virtual machine.	N/A
resume	ERROR	Replication ID	Failed to resume the replication synchronization for the replicated *vm-name* virtual machine.	A stack trace
reverse	INFO	Replication ID	The replication is reversed for the replicated *vm-name* virtual machine.	Warning messages and the reversed replication ID
reverse	ERROR	Replication ID	Failed to reverse the replication the replicated *vm-name* virtual machine.	A stack trace
reconfigure	INFO	Replication ID	The replication configuration is changed for the replicated *vm-name* virtual machine.	The new configuration and warning messages
reconfigure	ERROR	Replication ID	Failed to change the replication configuration for the replicated *vm-name* virtual machine.	A stack trace
reconfigureDisks	INFO	Replication ID	The replicated disks changed for the replicated *vm-name* virtual machine.	The replicated disks and warning messages

Table 2-4. Management Events (continued)

Event Type	Log Level	Resource ID	Description	Details
reconfigureDisks	ERROR	Replication ID	Failed to change the replicated disks for the replicated *vm-name* virtual machine.	A stack trace
pair	INFO	Site name	Paired to the *site-name* remote site.	Warning messages
pair	ERROR	Site name	Failed to pair to the *site-name* remote site.	A stack trace
repair	INFO	Site name	Updated the pairing to the *site-name* remote site.	Warning messages
repair	ERROR	Site name	Failed to update the pairing to the *site-name* remote site.	A stack trace
unpair	INFO	Site name	Broke the pairing with the *site-name* remote site.	Warning messages
unpair	ERROR	Site name	Failed to break the pairing with the *site-name* remote site.	A stack trace
policyChange	INFO	Replication Policy ID	The replication policy is changed.	The new policy

Table 2-5. Monitoring Events

Event Type	Log Level	Resource ID	Description	Details
lsConnectivity	ERROR	N/A	Failed to connect to the vCenter Server Lookup service.	A stack trace
dbConnectivity	ERROR	N/A	Failed to connect to the database.	N/A
ntpConnectivity	ERROR	N/A	Time is not synchronized with the NTP servers.	The NTP servers
managerConnectivity	ERROR	Manager Service ID	Failed to connect to the Manager Service.	Stack trace
vcdConnectivity	ERROR	N/A	Failed to connect to VMware Cloud Director.	A stack trace
tunnelConnectivity	ERROR	N/A	Failed to connect to the local Tunnel Service.	A stack trace
offlineRemoteSites	WARN	N/A	There are offline paired sites.	The site names
offlineLocalReplicators	WARN	N/A	There are offline local Replicator Service instances.	Replicator Service IDs
certExpiration	WARN	N/A	The certificate of the appliance expires in *number* days.	N/A
adminRemoteAccess	WARN	N/A	The administrative access is allowed from anywhere.	N/A
sshEnabled	WARN	N/A	The SSH access is enabled.	N/A
licenseExpired	WARN	N/A	The license is expired.	N/A

Table 2-5. Monitoring Events (continued)

Event Type	Log Level	Resource ID	Description	Details
replicationErrors	WARN	N/A	There are *number* replications with errors.	The replications IDs
rpoViolations	WARN	N/A	There are *number* replications with an RPO violation more than *number* minutes.	The replications IDs
offlineOnpremReplicators	WARN	N/A	There are offline On-Premises to Cloud Director Replication Appliance instances.	On-Premises to Cloud Director Replication Appliance IDs

Configure Provider Events

As a **service provider**, you can forward the VMware Cloud Director Availability provider events notifications to a syslog server, to VMware Cloud Director, or by using email delivery. All the delivery channels carry the same event information.

For more information about the events and notifications, see Events and Notifications.

Prerequisites

- Verify that VMware Cloud Director Availability 4.1 or later is deployed in the cloud site.
- To use the email delivery channel for events notifications, verify that you configured the SMTP settings in VMware Cloud Director. For more information, see Configure the System Email Settings in the *VMware Cloud Director Service Provider Admin Portal Guide*.

Procedure

1. Log in to the management interface of the Cloud Director Replication Management Appliance.
   a. In a Web browser, go to **`https://Appliance-IP-Address/ui/admin`**.
   b. Select **Appliance login** and enter the **root** user credentials.
   c. Click **Login**.
2. In the left pane, under **Configuration** click **Events and Notifications**.

   Note To forward provider events to the syslog server and to email, first you must configure these delivery channels. Without configuration, the **Syslog** and the **Cloud Director email** check boxes remain dimmed.

3 To configure the syslog server, under **Settings** next to **Syslog** click **Configure**.

   a In the **Syslog** window, enter the syslog server address and the UDP port.

   b To save the syslog configuration, click **Apply**.

4 (Optional) To configure the email notifications in the VMware Cloud Director Provider Portal, under **Settings** next to **Cloud Director Email** click the **Configure in Cloud Director** link.

   VMware Cloud Director Availability reads the following email settings from VMware Cloud Director:

   - The SMTP server configuration.
   - The sender email address.
   - The recipients of the email, either explicit email address or the email addresses of organization administrators.
   - The default subject prefix.

5 To configure the time before a given event is forwarded again, while the condition is still active, under **Settings** next to **Monitoring events forwarding time**, click **Edit**.

   The default **Monitoring events forwarding time** is 24 hours.

   a In the **Events configuration** window, under **Monitoring events forwarding time** enter the forwarding time.

   b To save the configuration for events notifications reposting, click **Apply**.

6 Under **Events** next to **System Management Events**, click **Edit**.

   a Next to **System Management Channels**, select **Syslog**, and or **Cloud Director events**, and or **Cloud Director email** as the notifications delivery channel.

   b To save the selected delivery channels, in the **System Management Events** window, click **Apply**.

7 Under **Events** next to **System Monitoring Events**, click **Edit** and to save the settings click **Apply**.

Option	Description
System Monitoring Channels	Select **Syslog**, and or **Cloud Director events**, and or **Cloud Director email** as the notifications delivery channel.
Connectivity poll interval	Time interval between polls for connectivity issues. The default value is 30 seconds.
Configuration poll interval	Time interval between polls for configuration issues. The default value is 1 day.
Certificate expiry threshold	The time before a certificate expires to start forwarding events. The default value is 30 days.
Policy compliance poll interval	The time between polls for policy compliance issues. The default value is 60 minutes.

8 Under **Events** next to **Replication Management Events**, click **Edit**.

   a Next to **Replication Management Channels**, select **Syslog** and or **Cloud Director events** as the notifications delivery channel.

   b To save the selected delivery channels, in the **Replication Management Events** window, click **Apply**.

9 Under **Events**, next to **Replication Monitoring Events** click **Edit** and to save the settings click **Apply**.

Option	Description
Replication Monitoring Channels	Select **Syslog**, and or **Cloud Director events**, and or **Cloud Director email** as the notifications delivery channel.
Poll interval	Time interval between polls for replication issues. The default value is 5 minutes.
RPO violation threshold time	Only forward events for replications with RPO violation time above this threshold. Use *0* to forward events for any RPO violation. The default value is 30 minutes.
RPO violation threshold time	Only forward events for replications with RPO violations count above this threshold. Use *0* to forward events for any number of replications with an RPO violation. The default value is 0.

Results

VMware Cloud Director Availability starts forwarding the events notifications to the selected delivery channels.

What to do next

You can monitor VMware Cloud Director Availability by using the syslog server, VMware Cloud Director, or your email client.

Configure Tenants Events

As a **service provider**, you can forward the VMware Cloud Director Availability tenant events notifications to VMware Cloud Director, or by using email delivery. Both delivery channels carry the same event information.

For more information about the events and notifications, see Events and Notifications.

Prerequisites

- Verify that VMware Cloud Director Availability 4.1 or later is deployed in the cloud site.
- To use the email delivery channel for events notifications, verify that you configured the SMTP settings in VMware Cloud Director. For more information, see Configure the System Email Settings in the *VMware Cloud Director Service Provider Admin Portal Guide*.

Procedure

1 Log in to the management interface of the Cloud Director Replication Management Appliance.

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

   b Select **Appliance login** and enter the **root** user credentials.

   c Click **Login**.

2 In the left pane, under **Configuration** click **Events and Notifications** and click **Tenants Events**.

3 From the **Organization** drop-down menu, select the organization for which you want to edit the events notifications configuration.

4 (Optional) To configure email notifications in the VMware Cloud Director Provider Portal, under **Settings** next to **Cloud Director Email** click **Configure in VCD**.

   VMware Cloud Director Availability reads the following email settings from VMware Cloud Director:

   - The SMTP server configuration.
   - The sender email address.
   - The recipients of the email, either explicit email address or the email addresses of organization administrators.
   - The default subject prefix.

5 Under **Events** next to **Replication Management Events**, click **Edit**.

   a Next to **Replication Management Channels**, select **Cloud Director events** as the notifications delivery channel.

   b To save the selected delivery channel, in the **Replication Management Events** window, click **Apply**.

6 Under **Events**, next to **Replication Monitoring Events** click **Edit** and to save the settings click **Apply**.

Note To forward tenant events by email, in VMware Cloud Director you must first configure the email delivery channel in step 3. Without email configuration, the **Cloud Director email** check box remains dimmed.

Option	Description
Replication Monitoring Channels	Select **Cloud Director events**, and or **Cloud director email** as the notifications delivery channel.
RPO violation threshold time	Only forward events for replications with RPO violation time above this threshold. Use *0* to forward events for any RPO violation. The default value is 30 minutes.
RPO violation threshold time	Only forward events for replications with RPO violations count above this threshold. Use *0* to forward events for any number of replications with an RPO violation. The default value is 0.

7 To restrict or allow the settings changes to the events notifications, modify the replication policy that is associated with the organization.

   For information about modifying the **Settings changes** in the replication policy, see Configuring Replication Policies in the *User Guide*.

Results

VMware Cloud Director Availability starts forwarding the tenants events notifications to the selected delivery channels.

What to do next

Tenants can monitor VMware Cloud Director Availability by using VMware Cloud Director, or their email client.

Bandwidth Throttling

In VMware Cloud Director Availability, you can set a global limit for the total incoming replication traffic from all remote cloud and on-premises sites. You can also configure a limit for the replication data traffic from on-premises sites to the cloud site. Throttling the network bandwidth can prevent the network saturation and avoid overloading of the management connections with replication data traffic sharing the network infrastructure.

In VMware Cloud Director Availability, throttling the network bandwidth to the specified megabits per second limits only the replication data traffic transfer rate. The bandwidth throttling does not limit the transfer rate of other types of network traffic like data and the management traffic.

Global Bandwidth Throttling for the Cloud Site

The global bandwidth throttling limits the transfer rate of the combined incoming replication data traffic to all local Replicator Appliance instances from all remote cloud or on-premises sites. This global traffic limit operates with any number of Replicator Appliance instances. The number of data connections or the activity within the connections has no effect on the bandwidth throttling.

On-Premises Bandwidth Throttling to the Cloud Site

The outbound network bandwidth throttling from on-premises sites to the cloud site applies to each individual On-Premises to Cloud Director Replication Appliance instance.

Configuring replication policies with an outbound bandwidth throttling limit for the traffic from on-premises appliances to the cloud site does not affect the traffic from a cloud site to a cloud site, nor affects the traffic from the cloud site to the On-Premises to Cloud Director Replication Appliance.

Configuring the organization replication policy with bandwidth throttling limit affects the transfer rate from all On-Premises to Cloud Director Replication Appliance instances, on all on-premises sites that target the respective organization.

Configure Bandwidth Throttling in the Cloud

To set a global limit for the incoming replication traffic from all peer sites, both remote cloud sites and on-premises sites, you can configure the bandwidth throttling for the cloud site.

For more information about the global bandwidth limit, see Bandwidth Throttling.

Procedure

1. Log in to the management interface of the Cloud Director 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 under **Configuration**, click **Settings**.
3. Under **Site settings** next to **Bandwidth throttling**, click **Edit**.
4. In the **Bandwidth throttling** window, configure the global limit for the incoming traffic from all peer sites.
   a. To enable bandwidth throttling, select the **Limit all incoming traffic** radio button.
   b. In the **Maximum mbit/s** text box, enter a numerical value for the replication traffic limit in megabits per second.
   c. From the **Tunnel nic** menu, select the Tunnel Appliance network adapter that is connected to the local site components.
   d. To save the settings, click **Apply**.

What to do next

You can also configure a limit for the replication data traffic from the on-premises sites to the cloud site. For more information, see Configure On-Premises Bandwidth Throttling to the Cloud.

Configure On-Premises Bandwidth Throttling to the Cloud

To set a limit for the replication data traffic from on-premises sites to the cloud site, configure the replication policies. All on-premises sites that target the organization to which this replication policy applies receive and apply this limit.

- Configuring the bandwidth throttling limit in the replication policy affects all On-Premises to Cloud Director Replication Appliance instances, on all on-premises sites that target the organization to which this replication policy applies. For more information about the bandwidth limit, see Bandwidth Throttling.
- For more information about the replication policies, see Configuring Replication Policies in the User Guide.

Procedure

1 Log in to the management interface of the Cloud Director 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 under **Configuration**, click **Policies**.
3 Select an existing replication policy and click **Edit**.
4 In the **Edit Policy** window under **General limits**, select **Enable bandwidth throttling**.
5 In the **Max throughput per On-Premises Replicator Appliance** text box, enter the limit in Mbit/s.
6 To save the bandwidth throttling limit, click **Apply**.

   Without re-pairing the on-premises sites, the bandwidth limit applies in 30 minutes.
7 In the list of policies, in the Maximum throughput column you can see the bandwidth limits for each policy.

Results

All On-Premises to Cloud Director Replication Appliance instances in the organization to which the replication policy applies receive and apply the bandwidth throttling limit that you configured.

What to do next

You can also configure a global limit for the total incoming replication traffic from all cloud sites. For more information, see Configure Bandwidth Throttling in the Cloud.

Backing Up and Restoring in the Cloud Director Site

Back up the cloud site and download the backup archive that contains appliance backup files for each appliance in the site. Restore the entire cloud site or only some of the appliances by restoring each appliance in a particular restore order by using its appliance backup file.

Backing Up the Cloud Site backed by VMware Cloud Director

Back up all the cloud appliances in the site by using the Cloud Director Replication Management Appliance management interface. Generating the backup allows downloading a backup archive `cloud-backup-product.version.build-site_name-date-timestampUTC.tar.bz2` file.

This backup archive contains the following information from each appliance in the cloud site:

- Configuration files
- Public certificate

- Keystore
- Database dump

In the backup archive `cloud-backup-`*`product.version.build-site_name-date-timestamp`*`UTC.tar.bz2` file, this information is stored as the multiple `.enc` appliance backup files:

- One `cloud-`*`backup_id`*`.tar.bz2.enc` appliance backup file for restoring the Cloud Director Replication Management Appliance.
- One or more `replicator-`*`backup_id-IP_Address`*`.tar.bz2.enc` appliance backup files for restoring each Replicator Appliance instance in the site.
- One `tunnel-`*`backup_id`*`.tar.bz2.enc` appliance backup file for restoring the Tunnel Appliance.

During the backup generation, the provided password encrypts all the `.enc` appliance backup files for preserving any sensitive information.

The backup does not contain:

- The appliance **root** user password.
- Any previous backup archives.
- Any support bundles.
- The NTP time server configuration.
- Enable SSH state.
- The network configuration provided in the OVF wizard during appliance deployment.
- Static routes configured on appliances with multiple network interface cards (NICs).

Restoring the Cloud Site

To restore a VMware Cloud Director Availability cloud site from a backup, use cloud appliances with matching:

- Version
- Appliance roles
- Network settings
- Number of appliances*

The `cloud-backup-`*`product.version.build-site_name-date-timestamp`*`UTC.tar.bz2` backup archive contains all the `.enc` appliance backup files that contain the backup information for each appliance in the site.

Follow the order and restore all of the appliances in the cloud site to the *date-timestamp* when the backup was generated, by browsing for the extracted `.enc` appliance backup files.

1 First, for restoring the Tunnel Appliance select the locally extracted `tunnel-backup_id.tar.bz2.enc` appliance backup file and provide the backup password.

2 Then, for restoring the Cloud Director Replication Management Appliance select the locally extracted `cloud-backup_id.tar.bz2.enc` appliance backup file and provide the backup password.

3 Last, for restoring each Replicator Appliance instance select each of the locally extracted `replicator-backup_id-IP_Address.tar.bz2.enc` appliance backup files and provide the backup password.

* VMware Cloud Director Availability 4.3 introduces in-place restore and restore of a single appliance in the cloud site.

In-place restore

In VMware Cloud Director Availability 4.3 or later, each appliance supports in-place restore and deploying a new appliance for restoring the backup is no longer necessary. Restoring in-place also does not require powering off of the appliance before the in-place restore.

Restore of a single cloud appliance

In VMware Cloud Director Availability 4.3 or later, if only a single cloud appliance in the site becomes irrecoverable by other means, you can restore only that appliance instead of restoring all the cloud appliances in the site. Restoring always requires an appliance with exactly the same version as the remaining cloud appliances in the site and with exactly the same version as the downloaded backup archive.

- Restoring a single cloud appliance, without restoring any of the remaining appliances in the site does not require following any restore order.
- Restoring several appliances from the site but not all cloud appliances, requires following the same restore order for restore as restoring the cloud site.
  a If restoring the Tunnel Appliance, restore it first.
  b If restoring the Cloud Director Replication Management Appliance, ensure that you follow the restore order.
    1 If restoring Tunnel Appliance as well, then restore the Cloud Director Replication Management Appliance after restoring the Tunnel Appliance.
    2 If restoring a Replicator Appliance instance as well, restore the Cloud Director Replication Management Appliance before that.

c If restoring a Replicator Appliance instance, restore it as last. If needed, repeat with restoring other Replicator Appliance instances.

Back up All Appliances in the Cloud

In the Cloud Service management interface, as a **service provider** you generate new backup archives of all the VMware Cloud Director Availability appliances in the cloud site. Download the backup archive as a file and then preserve it on an external storage device for future restore of the cloud site to that moment in time.

You generate a backup of all the VMware Cloud Director Availability appliances in the cloud site only by using the management interface of the Cloud Service. This backup archive contains the following information from each appliance in the cloud site:

- Configuration files
- Public certificate
- Keystore
- Database dump

In the backup archive, this information is stored as multiple `.enc` appliance backup files. When generating the backup, you provide a password that encrypts the `.enc` appliance backup files to preserve any sensitive information.

A backup file does not contain:

- The appliance **root** user password.
- Any previous backup archives.
- Any support bundles.
- The NTP time server configuration.
- Enable SSH state.
- The network configuration provided in the OVF wizard during appliance deployment.
- Static routes configured on appliances with multiple network interface cards (NICs).

Locally, the appliances can store up to 24 backup archives on their internal storage. Past that number, you must delete some of them, or attempting to create another backup, shows `Backup quota exceeded. Number of allowed backups: 24, current backup count: 24.` Such limit does not apply for the **Scheduled backup archives** that are stored on an external SFTP storage. For more information, see Schedule Backup Archives.

Note After evacuating a datastore, all backups taken priorly cannot restore the replications. For information about datastore evacuation, see Evacuate the Replication Data from a Datastore.

Prerequisites

- Verify that before taking a backup, all VMware Cloud Director Availability services are operational. As exception, unreachable Replicator Service instances without incoming replications do not prevent generating a backup.
- Verify that the `free disk space` value in the bottom of the **System health** page shows at least the following amount of free space for each of the VMware Cloud Director Availability appliances in the cloud site:
  - Cloud Director Replication Management Appliance 40%
  - Each Replicator Appliance instance 35%
  - Tunnel Appliance 35%

Procedure

1. Log in to the management interface of the Cloud Director 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 under the **System** section, click **Backup Archives**.
3. In the top right corner next to **Scheduled backup archives**, click **Manual backup archives**.
4. On the **Manual backup archives** page, to generate a backup archive click **Generate new**.
5. In the **Generate a new backup archive** window, generate the backup archive of the cloud site.
   a. In the **Password** text box, enter a password that protects and encrypts the backup archive contents.

      The password that you enter must contain a minimum of eight characters and must consist of:
      - At least one lowercase letter.
      - At least one uppercase letter.
      - At least one number.
      - At least one special character, such as & # % .

   b. In the **Confirm Password** text box, reenter the password to confirm the password that encrypts the backup.

      Note Store the backup password in a safe place since it cannot be restored later.

   c. To generate the backup archive, click **Generate**.

   In the **Backup archives** page, you can see the progress of generating the new backup archive.

6 To locally download a generated backup archive, in the Backup Id column click the ***backup id*** link.

   a In the **Download Backup Archive** window, to save the backup file locally click **Download**.

      In your Web browser, the archive `cloud-backup-`*`product.version.build-site_name-date-timestamp`*`UTC.tar.bz2` file starts downloading.

   b Store the locally downloaded backup archive and its password for future restore of the cloud site to that moment in time.

   The backup archive `cloud-backup-`*`product.version.build-site_name-date-timestamp`*`UTC.tar.bz2` file downloaded, providing a locally-stored backup point in time of the site.

7 (Optional) Remove a backup archive from the appliance.

   a Select one or more generated backup archives for removal and click **Delete**.

   b In the **Remove Archives** window, to confirm the removal click **Delete**.

      You deleted the selected backup archives from the appliance. For restoring, use a locally downloaded backup archive.

What to do next

You can later use a downloaded backup archive to restore all the VMware Cloud Director Availability appliances in the cloud site to that moment in time. For information about restoring from a backup archive, see Restore Appliances in the Cloud.

Restore Appliances in the Cloud

As a **provider**, you restore VMware Cloud Director Availability appliances in the cloud site on appliances with the same version, appliance role and network settings and by using a single appliance backup `.enc` file, extracted from the locally downloaded backup archive.

Note Restoring backups containing deleted replications at the time of restore:

In the management interface of a restored Replicator Service instance, on the **System Tasks** page the **Reload destination** tasks run indefinitely or fail with a `Lock acquisition timed out for object: 'H4-`*`id`*`'` for each replication that is not present since restoring the backup. To manually delete these replications, click the **Emergency Recovery** page, select them then click **Delete**.

- To restore a single appliance in the cloud site, depending on whether restoring on a newly deployed, or restoring in-place over the backed-up appliance:
  - When deploying a new appliance, power off the existing backed-up appliance in the site with the same role.
  - When restoring in-place over the backed-up appliance, without deploying a new appliance, do not power it off.

Restoring a single appliance does not require following the restore order and can be performed for any of the backed-up cloud appliances. For more information, see Backing Up and Restoring in the Cloud Director Site.

- To restore several of the appliances in the cloud site, but not all, follow the same restore order as with restoring the entire site. For more information, see Backing Up and Restoring in the Cloud Director Site.
- To restore an entire backed-up cloud site, restore the same number of appliances with matching appliance roles. For example, to restore a site consisting of a Tunnel Appliance, a Cloud Director Replication Management Appliance, and a couple of Replicator Appliance instances, you must restore a Tunnel Appliance, a Cloud Director Replication Management Appliance, and a couple of Replicator Appliance instances by following the restore order bellow.

The backup archive `cloud-backup-`*`product.version.build-site_name-date-timestamp`*`UTC.tar.bz2` file contains all of the following password-protected `.enc` appliance backup files for all of the cloud appliances in the site.

1 One `tunnel-`*`backup_id`*`.tar.bz2.enc` appliance backup file for firstly restoring the Tunnel Appliance.

2 One `cloud-`*`backup_id`*`.tar.bz2.enc` appliance backup file for then restoring the Cloud Director Replication Management Appliance.

3 One or more `replicator-`*`backup_id-IP_Address`*`.tar.bz2.enc` appliance backup files for lastly restoring each Replicator Appliance instance in the site.

These appliance backup files contain all the backup information for restoring each of the appliances in the cloud site to the *date-timestamp* point in time when the backup was generated. For more information, see Back up All Appliances in the Cloud.

To restore multiple appliances, repeat this procedure multiple times, according to the restore order and restore the appliances in the cloud site by using the appropriate appliance backup file for each appliance role, as extracted from the backup archive.

Prerequisites

- Verify that VMware Cloud Director Availability 4.3 or later is installed in the cloud site for in-place restore and for restore of a single or several cloud appliances, but not all appliances in the site.
- Verify that you have the backup password and that you locally extract the backup archive `cloud-backup-`*`product.version.build-site_name-date-timestamp`*`UTC.tar.bz2` file, resulting in several `.enc` appliance backup files, listed below.
- Verify that the following settings of the cloud appliance for restoring exactly match the backed-up appliance.
  - Version
  - Appliance role

  - Network settings
- Verify that before restoring on a newly deployed appliance, the existing backed-up appliance in the site with the same role is powered off.

  Caution Restoring on a newly deployed appliance while the existing backed-up appliance in the site with the same role is operational might corrupt the replications.

  However, for VMware Cloud Director Availability 4.3 or later, when restoring an appliance in-place, where the backed-up appliance matches the appliance on which you restore, do not power it off.

Procedure

1 Follow the restore order and log in to the VMware Cloud Director Availability appliances.

  a In a Web browser, go to the management interface of the VMware Cloud Director Availability appliances in the following restore order:

Restore Order	Appliance	Service	Management Interface
1	Tunnel Appliance	Tunnel Service	`https://Tunnel-Appliance-IP-Address/ui/admin`
2	Cloud Director Replication Management Appliance	Cloud Service	`https://Replication-Management-Appliance-IP-Address/ui/admin`
3	Each Replicator Appliance instance	Replicator Service instances	`https://Replicator-Appliance-IP-Address/ui/admin`

  b Log in by entering the **root** user password.

  If restoring on a newly deployed appliance, this is the password that you set during the OVA deployment.

2 If restoring on a newly deployed appliance, in the **VMware Cloud Director Availability Appliance Password** window, change the initial **root** user password.

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

  b Enter and confirm a new password. The password that you enter must be a secured password with a minimum of eight characters and it must consist of:

    - At least one lowercase letter.
    - At least one uppercase letter.
    - At least one number.
    - At least one special character, such as & # % .

3 Initiate restoring from the backup archive in the following restore order, according to the appliance role you restore.

   a Firstly, for the Tunnel Appliance, in the left pane under the **System** section, click **Backup Archives** then click **Restore**.

   b Secondly, repeat the same restore actions for the Cloud Director Replication Management Appliance.

   c Lastly, for each Replicator Appliance instance repeat the same restore actions.

4 Following the restore order of the appliances according to their role, browse for the appliance backup file, enter its password, and restore the appliance.

   a In the **Restore from a backup archive** window, click **Browse** and select the extracted `.enc` appliance backup file for the appliance role you are restoring.

      - First, for restoring the Tunnel Appliance select the `tunnel-`*`backup_id`*`.tar.bz2.enc` appliance backup file.
      - Then, for restoring the Cloud Director Replication Management Appliance select the `cloud-`*`backup_id`*`.tar.bz2.enc` appliance backup file.
      - Last, for restoring each Replicator Appliance instance select each of the `replicator-`*`backup_id-IP_Address`*`.tar.bz2.enc` appliance backup files.

   b In the **Password** text box, enter the password used for encrypting the backup.

   c To initiate the restoring of this appliance, click **Restore**.

      Restoring starts and might take a while until complete. While restoring is in progress, you cannot login to this appliance.

   After restoring completes, this appliance restarts.

5 (Optional) After the services start, verify that restoring is successful.

   a Log in to the management interface of the newly restored appliance.

   b In the left pane, click **System Tasks**.

      After the restore, the `Generate backup archive` task, which generated the backup archive used for the restore, shows `Task aborted due to service reboot`.

   c Verify the Target of `task.restore.backup`.

      For the Replicator Appliance instances, on the **System tasks** page, you see `Reload replication` tasks for each incoming replication of this Replicator Service instance.

Results

After repeating this procedure multiple times, you restored some or all of the cloud appliances in the site with matching appliance roles.

- The Tunnel Appliance is restored from the backup.

- The Cloud Director Replication Management Appliance is restored from the backup.
- All of the Replicator Appliance instances are restored from the backup.

Note

- After restore, there might be a misalignment between the replication settings stored in the database and the ones loaded from the backup file. As a result, you might see RPO violations, differing numbers of instances, and others, that you can resolve by reconfiguring the affected replications for reapplying their replication settings.
- After restoring, if an RPO violation is present, the replication might be missing from the source Replicator Service. This situation might happen when the source site is restored to a point in time when the replication is not yet started, leading to not working synchronization. As a workaround, you can attempt manually synchronizing the replication. If the synchronization task fails with `SourceReplicationNotFound`, fail over the replication, stop the replication, then deactivate the replication services for that virtual machine in the source ESXi host, see KB https://kb.vmware.com/s/article/2106946. Finally, start a new replication with a seed virtual machine.
- **Instances**

  After restore, the instances might disappear for some replications. In most cases, the data is not lost and a subsequent synchronization transfers only a delta. To get an instance, either wait for automatic synchronization, or perform a synchronization manually.
- After evacuating a datastore, all backups taken priorly cannot restore the replications. Take a backup every time the replications are moved from one datastore to another to ensure restoring is successful. For information about datastore evacuation, see Evacuate the Replication Data from a Datastore.

What to do next

You can perform replication workflows. After confirming that the restored appliances are operational, if you restored on a newly deployed appliances, you can decommission the backed-up appliances that are powered off.

Maintenance in the Cloud Director Site

In cloud sites backed by VMware Cloud Director, perform maintenance operations on a datastore, or on a Replicator Service instance, or rebalance replications across Replicator Service instances, or replace a Tunnel Appliance.

Evacuate the Replication Data from a Datastore

For performing maintenance operations on a local datastore in the cloud site evacuate all incoming replications and replication data placed on that datastore. To evacuate the replications

from the datastore at once, apply an alternative storage policy for all incoming replications that reside on the datastore.

Note

- Evacuating a datastore invalidates all VMware Cloud Director Availability backups created priorly and they cannot restore the replications.

  To ensure restoring from a backup is successful, create a backup every time the replications are moved from one datastore to another. For information about restoring, see Restore Appliances in the Cloud.

- Evacuating a datastore might take several hours until completed and depends on the amount of data for transferring.
- Since VMware Cloud Director Availability 4.4 evacuating replicas from individual members of datastore clusters is supported. Replications on a member datastore can move only to a different (for example, temporary) storage policy, they cannot be rebalanced within the other member datastores within the same cluster. After maintenance completes, the replications can be moved back from the temporary location to the original datastore cluster.

Prerequisites

Verify that VMware Cloud Director Availability 4.4 or later is deployed in the cloud site for evacuating datastore clusters.

Procedure

1 Log in to the management interface of the Cloud Director 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 under **System**, click **Datastores**.
3 (Optional) To show the replications that are placed on a datastore that displays replications counters, click **Preview**.

   For datastore clusters, expand to show the cluster members.
4 Select a local datastore or a cluster member that displays replications counters and click **Evacuate**.
5 In the **Evacuate datastore** window, select the destination storage policy for all incoming replications residing on the datastore and click **Evacuate**.
   - **Reset current storage policy** applies the current storage policy to each matching replication. After removing or adding datastores to the storage policy, to make the matching replications compliant with their storage policy this option can move the replication replica files.

- **Any** stores all the replications to all the shared datastores that have `Any` storage policy applied.
- ***pVDC Storage policy*** applies 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

VMware Cloud Director 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.

Replicator Service Maintenance Mode

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

The Replicator Service 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 Replicator Service instance in maintenance mode migrates all incoming cloud replications to other Replicator Service instances in the local site. Also, VMware Cloud Director 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 Replicator Service instance to other Replicator Service instances. Log in to the remote site and place in maintenance mode the same Replicator Service instance. Repeat this step in each remote site, where this Replicator Service instance is remotely registered.

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

Prerequisites

- Verify that VMware Cloud Director Availability is successfully deployed in the cloud site.
- Verify that more than one Replicator Service 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 the Replicator Service 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 Manager Service 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 Replicator Service instance and click **Enter Maintenance Mode**.
4. To evacuate the outgoing replications from this Replicator Service instance, log in to the Manager Service in the remote site and repeat this procedure.

   In the remote site, select the same Replicator Service instance that is remotely registered.

   Repeat step 4 for all cloud sites, where the Replicator Service instance is remotely registered.

Results

After placing a Replicator Service instance in maintenance mode from both the local site and all remote sites where it is registered, VMware Cloud Director Availability evacuates all replications from that Replicator Service instance. The Replicator Service 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 Replicator Service instance with replications, you must rebalance the replications. For more information, see Rebalance Replications.

Rebalance Replications

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

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

Prerequisites

- Verify that VMware Cloud Director Availability is successfully deployed in the site.
- Verify that more than one Replicator Service instance is operational in the site.

Procedure

1. Log in to the Manager Service 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

VMware Cloud Director Availability migrates and evenly distributes the replications to each operational Replicator Service instance in the site.

Replace a Tunnel Appliance

To replace or restore a failing Tunnel Appliance, power it off, deploy a new instance of the appliance and enable tunneling to the new appliance.

If VMware Cloud Director Availability 4.1 or later is deployed and a backup of the Tunnel Appliance exists, follow the procedure in Restore Appliances in the Cloud instead of the procedure below. To generate a backup in VMware Cloud Director Availability 4.1 or later, see Back up All Appliances in the Cloud.

Prerequisites

- Verify that VMware Cloud Director Availability is deployed in the cloud site.
- Verify that the existing Tunnel Appliance is powered off or that it is disconnected from the port group.

Procedure

1. Deploy a new Tunnel Appliance.
   a. Use the same host name, IP address, and the remaining settings as the original Tunnel Appliance.
   b. Power on the new Tunnel Appliance.

2 Log in to the Tunnel Service management interface.

   a In a Web browser, go to `https://Tunnel-IP-or-FQDN:8442`.

   b Select **Appliance login** and enter the **root** user password that you set during the OVA deployment.

   c Click **Login**.

3 If you log in to the appliance for the first time, you must change the initial **root** user password.

   a Enter the initial **root** user password that you set during the OVA deployment.

   b Enter and confirm a new password.

   The password that you enter must be a secured password with a minimum of eight characters and it must consist of:

   - At least one lowercase letter.
   - At least one uppercase letter.
   - At least one number.
   - At least one special character, such as & # %.

   c Click **Apply**.

   The **Getting Started** tab opens.

4 (Optional) To log in to the Tunnel Service by using vCenter Single Sign-On credentials, you can register the new Tunnel Appliance with the vCenter Server Lookup service.

   a In the **Configuration** page, under **Service endpoints**, next to **Lookup Service Address**, click **Edit**.

   b In the **Lookup Service Details** window, enter the **Lookup Service Address**.

   Pressing Tab autocompletes the vCenter Server Lookup service address to `https://Lookup-Service-IP-Address:443/lookupservice/sdk`.

   c Click **Apply**.

   d Verify the thumbprint and accept the certificate of the vCenter Server Lookup service.

5 Log in to the management interface of the Cloud Director 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 Enable tunneling to the new Tunnel Appliance.

   a In the left pane under **Configuration**, click **Settings**.

   b Under **Service endpoints**, next to **Tunnel Service address** click **Edit**.

c In the **Tunnel Service Settings** window, enter the **root** user password.

The **Tunnel Service Endpoint address** is already populated and the **Appliance user** is set to **root**.

d Click **Apply**.

e Verify the thumbprint and accept the certificate of the Tunnel Service.

Results

The new Tunnel Appliance starts tunneling for the VMware Cloud Director Availability services communication.

- For the paired cloud sites, you do not need to perform additional operations. In a few minutes, the pairing reports a green status and the replications proceed according to their RPO.
- For the paired on-premises sites, the Cloud Service reports a red status for all the pairings incoming from on-premises and outgoing to on-premises. The paired On-Premises to Cloud Director Replication Appliance instances continue to report a green status for pairing to cloud and the replications from on-premises to cloud proceed according to their RPO. To restore the replications from cloud to on-premises, you can restart the On-Premises to Cloud Director Replication Appliance instances or you can repair all on-premises sites with the cloud site.

What to do next

You can verify that all services are running correctly. For more information, see Verify the Uptime and the Local and the Remote Connectivity in the Cloud.

Uninstall VMware Cloud Director Availability from the Cloud Director Site

To remove a VMware Cloud Director Availability instance from a cloud site backed by VMware Cloud Director, stop the replications, delete pairing with all peer sites, remove both the plug-ins from vSphere and from VMware Cloud Director, then remove the cloud appliances.

When replacing an old VMware Cloud Director Availability instance, to prevent the error message `VM already protected` after installing the new VMware Cloud Director Availability instance, follow the steps in this procedure.

Prerequisites

Verify that VMware Cloud Director Availability is deployed in the cloud site backed by VMware Cloud Director.

Procedure

1 Stop all replications from and to the VMware Cloud Director Availability instance you are removing.

   a Log in to the VMware Cloud Director Availability instance that you are removing.

   b In the left pane, click **Incoming Replications**.

   c Select all the replications and click **Delete**.

   d Repeat this step in **Outgoing Replications** and delete all the replications.

2 Delete the established trust with all peer sites.

   a In the left pane under **Configuration**, click **Peer Sites**.

   b In the **Cloud sites** page, select a cloud site, then click **Delete**.

   c In the **Delete Peer Cloud Site** window, to delete the cloud site pairing, click **Delete**.

   You deleted the pairing with the cloud site and removed the trust from both the local and the remote cloud sites.

   d Repeat the above steps until you delete the pairing with all peer cloud sites.

   e Delete the established trust with all on-premises sites from the cloud site.

   - If the on-premises site is still paired, delete the pairing from the cloud site, then from the on-premises site delete the remaining pairing with the cloud site. For information about deleting pairing from the on-premises site, see Unpair a Site.
   - If from the on-premises site the cloud site is already unpaired, then delete the remaining record in the cloud site.

   f On the **Peer Sites** page, under **On-premises sites**, click **Delete**.

   g In the **Delete On-Premises Site** window, to delete the on-premises site pairing, click **Delete**.

   Above **On-premises sites** you see a green `On-Premises site deleted successfully.` message. You removed the cloud site trust with the on-premises site. If you performed this procedure from the cloud site first, in the on-premises site the cloud site still shows as paired. For more information, see Unpair a Site.

   h Repeat the above step until you delete pairing with all peer on-premises sites.

   You deleted all peer sites paired with this VMware Cloud Director Availability instance.

3 Remove the VMware Cloud Director Availability vSphere Client Plug-In registration.

   a In the left pane, click **Settings**.

   b Under **Service endpoints** next to **Lookup Service Address**, click **Remove**.

   c In the **Remove Lookup Service Registration** window, enter the single sign-on **administrator** user credentials and click **Remove**.

The vCenter Server Lookup service is unregistered from the appliance configuration. After logging out then logging in to vCenter Server, the VMware Cloud Director Availability vSphere Client Plug-In shows as unregistered from the vCenter Server instance.

4 Remove the VMware Cloud Director Availability plug-in from VMware Cloud Director.

   a In the left pane, click **Settings**.

   b Under **Service endpoints** next to **VMware Cloud Director Address**, click **Remove plugin**.

   c In the **Remove VCD UI plugin** window, click **Remove**.

5 If the management interface of VMware Cloud Director Availability is not available, remove the VMware Cloud Director Availability plug-in from VMware Cloud Director by using its Service Provider Admin Portal.

   a Go to `https://vcloud.example.com/provider` and log in to the Service Provider Admin Portal of VMware Cloud Director by using the **system administrator** user credentials.

   b From the top navigation bar, select **More > Customize Portal**.

   c Select the check box next to the name of the VMware Cloud Director Availability plug-in, then click **Delete**.

   d To confirm removing the plug-in, click **Save**.

6 For the VMware Cloud Director Availability instance you are removing, delete all the virtual machines of its appliances from the vCenter Server instance.

Results

This VMware Cloud Director Availability instance is now uninstalled from the cloud site backed by VMware Cloud Director.

What to do next

You can now install a new VMware Cloud Director Availability instance in the same cloud site.

Administration in On-Premises and Provider Site

3

After installing and configuring the VMware Cloud Director Availability appliance in the vCenter Server site, you can perform management and administrative tasks. The following tasks include changes to the provisioned environment and routine administration and maintenance procedures.

- **On-premises and Provider vCenter Server site:**

  In either:

  - a VMware Cloud Director Availability on-premises vCenter Server site
  - or in a provider VMware Cloud Director Availability cloud vCenter Server site,

  perform the following administration tasks in this current chapter by using the appliances management interface or in the disaster recovery infrastructure.

- **Cloud site backed by VMware Cloud Director:**

  For information about VMware Cloud Director Availability cloud sites, backed by VMware Cloud Director, see the Chapter 2 Administration in the Cloud Director Site chapter.

This chapter includes the following topics:

Stretching Layer 2 Networks On-Premises

To prepare on-premises sites for L2 stretch, first deploy NSX Autonomous Edge, then register it and configure its network adapters by using the On-Premises to Cloud Director Replication

Appliance. To complete the L2 stretch, in the cloud site, depending on the NSX version create the server L2 VPN session and then create the client L2 VPN session on-premises.

Important Verify that the prerequisites for NSX and for VMware Cloud Director in the cloud site are met and that you follow the steps in the procedure below in the correct order.

- For information about the L2 stretch, see Stretching On-Premises Layer 2 Networks in the Cloud.
  - For the prerequisites for NSX in the cloud site, see Create a Server L2 VPN Session with NSX in the Cloud.
  - For the prerequisites for NSX Data Center for vSphere in the cloud site, see Create a Server L2 VPN Session with NSX Data Center for vSphere in the Cloud.

Procedure Overview

Before stretching the L2 networks, ensure that you follow the procedure in the correct order:

1 Initially, prepare the on-premises site for L2 VPN with NSX Autonomous Edge:

Note This on-premises procedure only applies for on-premises sites not managed by NSX. If NSX manages the on-premises site, skip this on-premises section and its subsections and to create a client L2 VPN session and an L2 stretch follow the NSX documentation.

   a To allow for an L2 stretch on-premises, first deploy an NSX Autonomous Edge appliance. For more information, see Deploy an NSX Autonomous Edge Appliance On-Premises.

   b After deploying NSX Autonomous Edge on-premises, register the newly deployed NSX Autonomous Edge by using the On-Premises to Cloud Director Replication Appliance. For more information, see Register the NSX Autonomous Edge On-Premises.

   c After registering the NSX Autonomous Edge, configure its network adapters by using the On-Premises to Cloud Director Replication Appliance. For more information, see Configure the Networks of the NSX Autonomous Edge On-Premises.

2 Complete the L2 stretch from on-premises to the cloud site by creating the server and the client VPN sessions:

   a After configuring the NSX Autonomous Edge on-premises, in the cloud site use its IP address when creating the server L2 VPN session. Depending on the NSX version in the cloud site, follow the correct procedure:

      - When using NSX in the cloud site, see Create a Server L2 VPN Session with NSX in the Cloud.
      - When using NSX Data Center for vSphere in the cloud site, see Create a Server L2 VPN Session with NSX Data Center for vSphere in the Cloud.

b Finally, complete the L2 stretch by using the On-Premises to Cloud Director Replication Appliance. For more information, see Create a Client L2 VPN Session On-Premises.

- Deploy an NSX Autonomous Edge Appliance On-Premises

  On-premises sites or the clients L2 VPN require a specially configured VMware® NSX Edge™ appliance called autonomous edge. Deploy the NSX Autonomous Edge appliance by using an OVF file on the ESXi host.

- Register the NSX Autonomous Edge On-Premises

  On-premises sites or the clients L2 VPN require a VMware® NSX Edge™ appliance configured as an autonomous edge. Once deployed in the on-premises site, the On-Premises to Cloud Director Replication Appliance starts managing the NSX Autonomous Edge after you register it on-premises.

- Configure the Networks of the NSX Autonomous Edge On-Premises

  After registering the NSX Autonomous Edge with the On-Premises to Cloud Director Replication Appliance, to connect to the NSX Edge in the cloud site configure the network adapters and the uplink port of the NSX Autonomous Edge on-premises.

- Create a Client L2 VPN Session On-Premises

  After configuring the networks of the NSX Autonomous Edge, by using On-Premises to Cloud Director Replication Appliance create the client side of the L2 VPN session, stretching one or more networks across the cloud site.

Deploy an NSX Autonomous Edge Appliance On-Premises

On-premises sites or the clients L2 VPN require a specially configured VMware® NSX Edge™ appliance called autonomous edge. Deploy the NSX Autonomous Edge appliance by using an OVF file on the ESXi host.

In on-premises data centers, you deploy an NSX Autonomous Edge and configure it as on-premises client side of an L2 VPN that connects to the cloud site.

Prerequisites

- Verify that VMware Cloud Director Availability 4.2 or later is successfully deployed.
- Verify that you have access to the NSX Edge OVF file.

Procedure

1. Locate the NSX Edge OVF file on the VMware download portal and either copy the download URL or download it locally.
2. By using the vSphere Client, log in to the vCenter Server that manages the non-NSX on-premises site.
3. Select **Hosts and Clusters** and to show the available hosts, expand the clusters.

4 To deploy the NSX Edge, right-click the host where you want it and select **Deploy OVF Template**.

   a On the **Select an OVF template** page, to download and deploy the OVF file, paste the URL, or select a locally downloaded OVF file and click **Next**.

   b On the **Select a name and folder** page, in the **Virtual machine name** text box enter a name for the NSX Autonomous Edge, select a location for its virtual machine and click **Next**.

   c On the **Select a compute resource** page, select the destination compute resource and click **Next**.

   d On the **Review details** page, verify the OVF package template details and click **Next**.

   e On the **Configuration** page, select a deployment configuration size and click **Next**.

   f On the **Select storage** page, select the provisioning, a storage for the configuration and the disk files and click **Next**.

   g On the **Select networks** page, for all destination networks select the management network and click **Next**.

   After the setup completes, the On-Premises to Cloud Director Replication Appliance takes over managing the network interfaces of the NSX Autonomous Edge. For more information, see Configure the Networks of the NSX Autonomous Edge On-Premises.

h On the **Customize template** page, enter the following properties and click **Next**.

Note The NSX Edge appliance does not validate the property values such as the passwords before powering on for the first time.

Option	Description
System Root User Password	Enter and confirm the passwords for the system users, that meet the following complexity requirements: ■ At least 12 characters ■ At least one uppercase letter ■ At least one lowercase letter ■ At least one digit ■ At least one special character ■ At least five different characters ■ No dictionary words ■ No palindromes ■ No more than four monotonic character in a sequence **Note** NSX Edge core services do not start unless you enter passwords meeting these requirements.
CLI "admin" User Password	
Is Autonomous Edge	Select this property to deploy the NSX Edge node as an autonomous edge in the L2 VPN topology. NSX does not manage NSX Edge nodes determined as autonomous edges.

- You can enable SSH and allow **root** SSH login.
- Skip configuring the remaining properties, like hostname or IP.

i On the **Ready to complete** page, review the NSX Autonomous Edge settings and click **Finish**.

5 After the deployment completes, power on the NSX Autonomous Edge virtual machine.

Results

The NSX Autonomous Edge appliance deployed successfully on-premises.

What to do next

Register this newly deployed NSX Autonomous Edge for L2 stretch management by using the management interface of the On-Premises to Cloud Director Replication Appliance. For more information, see Register the NSX Autonomous Edge On-Premises.

Register the NSX Autonomous Edge On-Premises

On-premises sites or the clients L2 VPN require a VMware® NSX Edge™ appliance configured as an autonomous edge. Once deployed in the on-premises site, the On-Premises to Cloud

Director Replication Appliance starts managing the NSX Autonomous Edge after you register it on-premises.

To complete the L2 stretch configuration entirely by using the management interface of the On-Premises to Cloud Director Replication Appliance, after deploying the NSX Autonomous Edge in the on-premises site you register it by using the On-Premises to Cloud Director Replication Appliance.

Prerequisites

- Verify that VMware Cloud Director Availability 4.2 or later is successfully deployed.
- Verify that the On-Premises to Cloud Director Replication Appliance is paired with a cloud site. All L2 stretch settings on-premises enable only after pairing with a cloud site as the On-Premises to Cloud Director Replication Appliance must browse the virtual machines.
- Verify that an NSX Edge appliance is deployed on-premises, selected as an autonomous edge and configured with passwords for the **root** and the **admin** users that meet the complexity requirements. For more information, see Deploy an NSX Autonomous Edge Appliance On-Premises.

Procedure

1. Log in to the management interface of the VMware Cloud Director Availability On-premises Appliance.
   a. In a Web browser, go to `https://On-Premises-Appliance-IP-address/ui/admin`.
   b. Log in as the **root** user.
2. In the left pane, under the **System** section click **L2 Stretch**.
3. On the **NSX Autonomous edges** page, click **New**.
4. In the **Register a New NSX Autonomous Edge** window, register the new NSX Autonomous Edge with the On-Premises to Cloud Director Replication Appliance.
   a. In the **Name** text box, enter a friendly name for the new NSX Autonomous Edge.
   b. From the **vCenter Server** drop-down menu, select thevCenter Server instance hosting the NSX Autonomous Edge virtual machine.
   c. Under **NSX Autonomous Edge VMs**, select the virtual machine of the newly deployed NSX Autonomous Edge.
   d. In the **Management Address** text box, enter the URL for the NSX Autonomous Edge management.
   e. In the **User name** and **Password** text boxes, enter the **admin** user credentials for the NSX Autonomous Edge management.
   f. (Optional) In the **Description** text box, enter a description for this NSX Autonomous Edge.
   g. To register the NSX Autonomous Edge for management, click **Register**.

Results

The On-Premises to Cloud Director Replication Appliance registered the new NSX Autonomous Edge for L2 stretch management.

What to do next

You can now configure the networks of the newly registered NSX Autonomous Edge by using the On-Premises to Cloud Director Replication Appliance. For more information, see Configure the Networks of the NSX Autonomous Edge On-Premises.

Configure the Networks of the NSX Autonomous Edge On-Premises

After registering the NSX Autonomous Edge with the On-Premises to Cloud Director Replication Appliance, to connect to the NSX Edge in the cloud site configure the network adapters and the uplink port of the NSX Autonomous Edge on-premises.

During the NSX Autonomous Edge deployment, its four network adapters are configured with the management network. For more information, see Deploy an NSX Autonomous Edge Appliance On-Premises. For the L2 stretch to operate, by using the management interface of the On-Premises to Cloud Director Replication Appliance configure the network adapters and the uplink port of the NSX Autonomous Edge on-premises.

Prerequisites

- Verify that VMware Cloud Director Availability 4.2 or later is successfully deployed.
- Verify that the On-Premises to Cloud Director Replication Appliance is paired with a cloud site. All L2 stretch settings on-premises enable only after pairing with a cloud site as the On-Premises to Cloud Director Replication Appliance must browse the virtual machines.
- Verify that the NSX Autonomous Edge in the on-premises site is powered on and registered with the On-Premises to Cloud Director Replication Appliance. For more information, see Register the NSX Autonomous Edge On-Premises.

Procedure

1. Log in to the management interface of the VMware Cloud Director Availability On-premises Appliance.
   a. In a Web browser, go to `https://On-Premises-Appliance-IP-address/ui/admin`.
   b. Log in as the **root** user.
2. In the left pane, under the **System** section click **L2 Stretch**.
3. On the **NSX Autonomous edges** page, select a newly deployed NSX Autonomous Edge instance.
4. Click **Edit network**.

5 In the **Configure the NSX Autonomous Edge Network Adapters** window, configure the network adapters of the NSX Autonomous Edge and click **Apply**.

   Cannot select the **Management Network** of the NSX Autonomous Edge preventing the loss of connectivity to it.

   a From the **VLAN Trunk Network** drop-down menu, to allow intercepting the on-premises network traffic for the L2 stretch networks by VMware Cloud Director Availability, select a network or a port group allowing VLAN trunking.

   b From the **Uplink Network** drop-down menu, to allow the external communication, select a network that can connect to the cloud site NSX Edge.

6 With the newly deployed NSX Autonomous Edge selected, click **Configure the uplink port**.

7 In the **Configure the Uplink Port** window, enter the settings for the external network port and click **Apply**.

   a In the **IP Address/Prefix** text box, enter the IP address and the subnet mask of the uplink port.

   b In the **VLAN** text box, enter the VLAN of the uplink port.

      - If not using a VLAN port group, enter 0.
      - If using a VLAN port group, it must be within the uplink network connected to the NSX Autonomous Edge.

   c (Optional) In the **MTU** text box, enter the maximum transmission unit (MTU) of the uplink port or leave the default MTU value of 1500 bytes.

   d (Optional) In the **Gateway** text box, enter a gateway for the uplink port.

Results

The On-Premises to Cloud Director Replication Appliance configured the NSX Autonomous Edge network on-premises.

What to do next

You can now create a server L2 VPN session by using the static endpoint IP address of this newly configured NSX Autonomous Edge. For more information, see Create a Server L2 VPN Session with NSX in the Cloud.

Create a Client L2 VPN Session On-Premises

After configuring the networks of the NSX Autonomous Edge, by using On-Premises to Cloud Director Replication Appliance create the client side of the L2 VPN session, stretching one or more networks across the cloud site.

Prerequisites

- Verify that VMware Cloud Director Availability 4.2 or later is successfully deployed.

- Verify that the On-Premises to Cloud Director Replication Appliance is paired with a cloud site. All L2 stretch settings on-premises enable only after pairing with a cloud site as the On-Premises to Cloud Director Replication Appliance must browse the virtual machines.
- Verify that in the cloud site the server L2 VPN session is created. For more information, see Create a Server L2 VPN Session with NSX in the Cloud.
- Verify that in the on-premises site the networks of the NSX Autonomous Edge are configured. For more information, see Configure the Networks of the NSX Autonomous Edge On-Premises.

Procedure

1 Log in to the management interface of the VMware Cloud Director Availability On-premises Appliance.

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

   b Log in as the **root** user.

2 In the left pane, under the **System** section click **L2 Stretch**.

3 On the **NSX Autonomous edges** page, click **L2 VPN Sessions**.

4 If more than one NSX Autonomous Edge instance is registered with the On-Premises to Cloud Director Replication Appliance, from the **NSX Autonomous Edge** drop-down menu, select the correct NSX Autonomous Edge name to use for the client L2 VPN session.

5 To create a client L2 VPN session, click **New** and complete the **New Client L2 VPN Session** wizard.

   If your user session is not currently extended to the cloud site, enter credentials to authenticate to the cloud site.

6 On the **VDC and edge Gateway** page, select the cloud site virtual data center and the edge gateway.

7 On the **Settings and networks** page, configure the L2 VPN and click **Next**.

   a In the **Name** text box, enter a name for this client L2 VPN session.

   b From the **Server session** drop-down menu, select the cloud side L2 VPN server session.

   c In the **Local Address** text box, enter the on-premises IP address at the client side of the L2 VPN session.

      The local IP address must be the same as the uplink port IP address of the NSX Autonomous Edge hosting the client L2 VPN session.

d In the **Remote Address** text box, enter the cloud IP address at the server side of the L2 VPN session.

Usually the remote IP address is the endpoint IP address of the server L2 VPN session. For more information, see Create a Server L2 VPN Session with NSX in the Cloud.

e Under the Client Network column, to create an L2 stretch across the networks select an on-premises VLAN network against each server network in the cloud site.

The number of available client networks for selection, depends on the cloud site version of VMware Cloud Director. For information about the versions of VMware Cloud Director, see the prerequisites in Create a Server L2 VPN Session with NSX in the Cloud.

8 On the **Ready To Complete** page, to create the L2 VPN stretch click **Finish**.

Results

The client L2 VPN session on-premises is created and the L2 stretch across the cloud site is complete.

What to do next

You can now use this stretched network when migrating some virtual machines to the cloud that are a part of a single on-premises workload, keeping the network connectivity between the migrated virtual machines in the cloud site and the non-migrated virtual machines on-premises. You can easily manage the L2 stretch by using the management interface of the On-Premises to Cloud Director Replication Appliance, or directly by using the management interface of the NSX Autonomous Edge.

Back up the Appliance

In the appliance management interface, you generate new a appliance backup archive. Download the backup archive as a file and then preserve it on an external storage device for future restore of the stack to that moment in time.

Since VMware Cloud Director Availability 4.4, backing up the On-Premises to Cloud Director Replication Appliance can be allowed from the cloud site. Backing up the On-Premises to Cloud vCenter Replication Appliance or the vCenter Replication Management Appliance can only be performed locally from the appliance.

This backup archive contains the following information from the appliance:

- Configuration files
- Public certificate
- Keystore
- Database dump

This information is stored as an `.enc` appliance backup file. When generating the backup, you provide a password that encrypts the appliance backup file to preserve any sensitive information.

The backup does not contain:

- The appliance **root** user password.
- Any previous backup archives.
- Any support bundles.
- The time server configuration.

Locally, the appliances can store up to 24 backup archives on their internal storage. Past that number, you must delete some of them, or attempting to create another backup, shows `Backup quota exceeded. Number of allowed backups: 24, current backup count: 24.` Such limit does not apply for the **Scheduled backup archives** that are stored on an external SFTP storage. For more information, see Schedule Backup Archives.

Prerequisites

- Verify that before taking a backup, the appliance is operational.
- Verify that the `free disk space` value in the bottom of the **System health** page shows at least 35%.

Procedure

1. Log in to the management interface of the VMware Cloud Director Availability 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 **Backup Archives**.
3. In the **Backup archives** page, click **Generate new**.
4. In the **Create backup archive** window, create a backup archive of the appliance.
   a. In the **Password** text box, enter the password to protect and encrypt the backup archive.

      The password that you enter must be a secured password with a minimum of eight characters and it must consist of:

      - At least one lowercase letter.
      - At least one uppercase letter.
      - At least one number.
      - At least one special character, such as & # % .

   b. In the **Confirm Password** text box, reenter the password to confirm the password that encrypts the backup.

c Store this password in a safe place since it cannot be restored later.

d Click **Create**.

In the **Backup archives** page, you see the progress of generating the new backup archive.

5 To download one of the generated backup archives, in the Backup Id column, click the ***backup id*** link.

a In the **Download Backup Archive** window, to save the backup file locally click **Download**.

In your Web browser, the `on-premises-backup-product_version-instance_id-date-timestampUTC.tar.bz2.enc` file starts downloading.

b Store the locally downloaded backup file and its password for future restore of the appliance to that moment in time.

Results

The appliance backup `on-premises-backup-product_version-instance_id-date-timestampUTC.tar.bz2.enc` file downloaded locally.

What to do next

You can later use one of the locally downloaded backup files to restore the appliance to that moment in time. For more information, see Restore the Appliance.

Restore the Appliance

You restore the appliance on-premises, by deploying a new on-premises appliance with the same network settings and by using a single locally downloaded `.enc` backup file.

Note Restoring backups containing deleted replications at the time of restore:

Go to the management interface of the restored appliance at `https://Appliance-IP-Address:8043`. On the **System Tasks** page or the **Replication Tasks** page, the **Reload destination** tasks run indefinitely or fail with a `Lock acquisition timed out for object: 'H4-id'` for each replication that is not present since restoring the backup. To manually delete these replications, click the **Emergency Recovery** page, select them then click **Delete**.

Prerequisites

- Verify that you downloaded the `on-premises-backup-product_version-instance_id-date-timestampUTC.tar.bz2.enc` file locally and you have the password for the backup.
- Verify that the version and the network settings of the newly deployed appliance exactly match the version and the network settings of the backed-up appliance.
- Verify that before restoring the newly deployed appliance, the existing backed-up on-premises appliance is powered off.

  Caution Restoring while the appliance is operational may corrupt the replications.

The `on-premises-backup-`*`product_version-instance_id-date-timestamp`*`UTC.tar.bz2.enc` file contains all the backup information to restore the appliance to the *date-timestamp*. For information about taking a backup, see Back up the Appliance.

Procedure

1 Log in to management interface of the newly deployed appliance.
   a In a Web browser, go to `https://`*`Appliance-IP-Address`*`/ui/admin`.
   b Log in by entering the **root** user password that you set during the OVA deployment.
2 In the **VMware Cloud Director Availability Appliance Password** window, change the initial **root** user password.
   a Enter the **root** user password that you set during the OVA deployment.
   b Enter and confirm a new password. The password that you enter must be a secured password with a minimum of eight characters and it must consist of:
      - At least one lowercase letter.
      - At least one uppercase letter.
      - At least one number.
      - At least one special character, such as & # % .
3 Under **Steps to restore from archive**, click **Import the backup archive in...**.
4 In the **Restore from backup archive** window, browse for the appliance backup file, enter its password, and restore the appliance.
   a Click **Browse** and select the locally downloaded `.enc` appliance backup file.
   b In the **Password** text box, enter the password used to encrypt the backup.
   c Click **Restore**.

      The restore starts and might take a while to complete. You cannot log in to the appliance while the restore is in progress.

   After the restore completes, the appliance restarts.
5 (Optional) After the services start, verify that the restore is successful.
   a Log in to the management interface of the newly restored appliance.
   b In the left pane, click **System Tasks**.

      After restore, the `Generate backup archive` task, which generated the backup archive used for the restore, shows `Task aborted due to service reboot`.
   c Verify the Target of `task.restore.backup`.

Results

A misalignment between the replication settings stored in the database and the ones loaded from the backup might happen. As a result, RPO violations, instances with differing numbers, and others might be present. As a resolution, reapply the replication settings by reconfiguring the affected replications .

Note

Instances

After restore, the instances might disappear for some replications. In most cases, the data is not lost and a subsequent synchronization transfers only a delta. To get an instance, either wait for automatic synchronization, or perform a synchronization manually.

What to do next

You can perform replication workflows and after confirming that the newly restored appliance is operational, you can decommission the backed-up appliance that is powered off.

Repair a Site

To reestablish the trust with a remote site, repair with the remote site by using the management interface of the appliance.

This procedure applies for the following appliance roles:

- On-Premises to Cloud Director Replication Appliance, see step 2.
- On-Premises to Cloud vCenter Replication Appliance, see step 3.

  After upgrading to version 4.5 both the On-Premises to Cloud vCenter Replication Appliance andvCenter Replication Management Appliance, the tenant must re-pair with the provider site.

  The on-premises appliance no longer requires a public URL and supports a single-step pairing to the provider site. The pairing from on-premises to a provider no longer requires additional steps for confirming the pairing from the provider site.
- vCenter Replication Management Appliance, see step 3.

Prerequisites

Verify that for vSphere DR and migration, both sites are upgraded to version 4.5 before re-pairing.

Procedure

1 Log in to the management interface of the VMware Cloud Director Availability 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 To re-pair, depending on the appliance role and the remote site choose the appropriate repair method and complete the pairing step.

   - For vSphere DR and migration, to re-establish the trust between vCenter Server sites skip this step and complete step 3.
   - Alternatively, to re-establish the trust with a cloud site backed by VMware Cloud Director follow this step and skip step 3.

   a In the left pane, click **Settings**.

   b Under **Site settings** next to **Pairing**, click **Repair** then complete the **Update Pairing** wizard.

   c On the **Site Details** page, verify this on-premises site name and description then click **Next**.

   d On the **Lookup Service** page, enter the **`single sign-on`** user credentials for the local vCenter Server Lookup service in the on-premises site then click **Next**.

e On the **Cloud Service Details** page, enter the credentials of the VMware Cloud Director **organization administrator** user, and to allow the cloud site permissions, toggle the cloud access and log collection then click **Next**.

Option	Description
Public Service Endpoint address	Enter the address of the cloud site's Service Endpoint:443 as provided by the cloud provider.
Organization Admin	Enter the user name of a VMware Cloud Director **organization administrator** user. For example, use ***admin@org***.
Organization Password	Enter the ***password*** of the VMware Cloud Director **organization administrator** user.
Allow access from Cloud	**Activated access from the cloud site:** Allows privileged VMware Cloud Director users like the cloud provider and the organization administrators without authenticating to the on-premises site to perform operations from the VMware Cloud Director Availability Tenant Portal: ■ Browse and discover on-premises workloads to replicate them to the cloud site. ■ Reverse existing replications from the cloud site to the on-premises site. ■ Replicate cloud site workloads to the on-premises site. **Deactivated cloud site access:** ■ Configuring a new replication requires users to explicitly authenticate to the on-premises VMware Cloud Director Availability Tenant Portal. ■ Cannot reverse existing replications to the on-premises site. ■ Allows privileged VMware Cloud Director users to modify existing replications and perform migrate or failover.
Allow log collection from Cloud	■ To simplify troubleshooting, activate log collection from the cloud site. This allows the cloud provider and the organization administrators without authenticating to each paired on-premises appliance to obtain its logs. ■ Leave cloud site log collection deactivated to require authenticating to the on-premises appliance management interface for downloading the on-premises appliance logs.

If the cloud site does not use a valid CA-signed certificate, verify the thumbprint and accept the SSL certificate of the Service Endpoint.

f On the **Ready to Complete** page, optionally, reconfigure the on-premises local placement, and to complete the wizard click **Finish**.

- You can use the existing placement of the on-premises replications by leaving the **Configure local placement now** toggle deactivated.
- To reconfigure the cloud to on-premises placement, activate the **Configure local placement now** toggle then complete the **Configure Placement** wizard.

3 Alternatively, to re-establish the trust with the remote vCenter Server site, complete this step.

On-premises to provider pairing is managed only from the on-premises site.

a In the left pane, click **Peer Sites**.

b To re-pair, select the site and click **Repair**.

c In the **Update Pairing** window, depending on which appliance initiates the repair, enter the following pairing details then click **Update**.

- As a **tenant**, initiate and complete the repair only from the On-Premises to Cloud vCenter Replication Appliance. The On-Premises to Cloud vCenter Replication Appliance does not require a publicly available address.

Option	Description
Public Service Endpoint	■ Enter the address of the Public Service Endpoint **:443** of the vCenter Replication Management Appliance. ■ Alternatively, enter port **8048** when both appliances reside in the same network.
SSO Username	Enter the user name of the single-sign-on user from the provider site for the pairing. For example, enter **Administrator@vsphere.local**. To pair the on-premises appliance with the provider site it is recommended to use a less-privileged user that belongs to the **VRUSERS** group in the provider site. Alternatively, you can still use a user member of the **VRADMINISTRATORS** or the **ADMINISTRATORS** groups in the provider site. For information about these groups, see Users Roles Rights and Sessions in the *Security Guide*.
SSO Password	Enter the password of the remote single-sign-on user in the provider site.
Description	Optionally, enter a description for this pair.

- As a **provider**, when repairing vCenter Replication Management Appliance with vCenter Replication Management Appliance, initiate the pairing by entering:

Option	Description
Public Service Endpoint	■ Enter the address of the vCenter Replication Management Appliance **:443**. ■ Alternatively, enter port **8048** when both appliances reside in the same network.
Description	Optionally, enter a description for this pair.

When repairing two vCenter Replication Management Appliance instances, after initiating pairing from the local site, to complete the pairing log in the remote vCenter Replication Management Appliance and repeat this step to also repair the remote site with the local vCenter Replication Management Appliance.

d Verify the thumbprint and accept the SSL certificate of the remote appliance.

4 Verify that the connectivity to the paired site is operational.

   a In the left pane, click **System Health**.

   b Verify that for the site you re-paired, **Service connectivity** shows a green `OK` status.

Results

The pairing between the local and the remote site is re-established.

Unpair a Site

To remove the established trust between the local site and a remote site, unpair the remote site from the local site by using the appliance management interface.

This procedure applies for the following appliance roles:

- On-Premises to Cloud Director Replication Appliance, see step 2.
- On-Premises to Cloud vCenter Replication Appliance, see step 3.
- vCenter Replication Management Appliance, see step 4.

Prerequisites

Delete all configured replications between the local site and the remote site.

Procedure

1 Log in to the management interface of the VMware Cloud Director Availability 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 Remove the established trust between the On-Premises to Cloud Director Replication Appliance and the cloud site backed by VMware Cloud Director.

   - If this On-Premises to Cloud Director Replication Appliance is still paired with the cloud site, first, from the on-premises site unpair the cloud site, then similarly from the cloud site, delete the remaining on-premises site pairing.

- If from the cloud site this On-Premises to Cloud Director Replication Appliance pairing is already deleted, remove the remaining pairing record in the on-premises site. When done, you see a red `Peer site 'on-prem-site-name' was not found` message because the remote site pairing is removed already.

a In the left pane, click **Settings**.

b Under **Site details** next to **Pairing**, click **Delete**.

c In the **Unpair from cloud site** window, enter the user credentials of the VMware Cloud Director **organization administrator** then click **Apply**.

The **Pairing** section shows `Not configured` and the cloud site registration is removed.

3 Remove the established trust between the On-Premises to Cloud vCenter Replication Appliance and the cloud site.

a In the left pane, click **Peer Sites**.

b Select the cloud site and click **Delete**.

4 Remove the established trust between two vCenter Replication Management Appliance instances.

a In the left pane, click **Peer Sites**.

b Select the remote site and click **Delete**.

c To delete the remaining pairing record, log in to the remote site and repeat this step.

Results

The pairing between this local site and the remote site is removed.

What to do next

- If you performed this procedure from the on-premises site first, in the cloud site backed by VMware Cloud Director the on-premises site still shows as paired. After unpairing the on-premises site, the **service provider** can remove the remaining record from the cloud site for the unpaired on-premises site. For more information, see Unpair paired sites from the cloud backed by VMware Cloud Director.
- You can remove the established connection between the on-premises appliance and vCenter Server, see Unregister the VMware Cloud Director Availability vSphere Client Plug-In.
- You can repair with the remote site, see Repair a Site.

Replace the Certificate of the Appliance

In an on-premises or in a cloud vCenter Server site, to replace the SSL certificate of the VMware Cloud Director Availability appliance, use its service management interface.

This procedure applies for the following appliance roles:

- **VMware Cloud Director Availability On-Premises Appliance roles:**
  - On-Premises to Cloud Director Replication Appliance
  - On-Premises to Cloud vCenter Replication Appliance

and for

- vCenter Replication Management Appliance

For information about replacing the certificates in a cloud site backed by VMware Cloud Director, see Certificates Management.

Procedure

1 Log in to the management interface of the VMware Cloud Director Availability 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 **Settings**.
3 Under **Appliance settings**, next to **Certificate** replace the appliance certificate and click **Apply**.
   - To import an SSL certificate, click **Import** and in the **Import Certificate** window, enter the certificate details.
   a Enter the password that protects the keystore and the certificate private key.
   b Click **Browse** and select the PKCS#12 file.
   - Alternatively, to generate a new self-signed certificate, click **Regenerate**.

   After replacing the certificate, the VMware Cloud Director Availability services that run in the appliance restart.
4 After replacing the certificate, redeploy the VMware Cloud Director Availability vSphere Client Plug-In by reapplying the vCenter Server Lookup service address.
   a Under **Service endpoints**, next to **Lookup Service Address** click **Edit**.
   b Enter the single-sign-on user credentials and click **Apply**.

Option	Description
SSO Admin Username	Enter the vSphere **administrator** user name for the vCenter Server Lookup service that belongs to the **ADMINISTRATORS** group.
Password	Enter the vSphere **administrator** user password for the vCenter Server Lookup service.

5 After replacing either or both of their certificates, repair the On-Premises to Cloud vCenter Replication Appliance and the vCenter Replication Management Appliance.

Skip this step after replacing the certificate of the On-Premises to Cloud Director Replication Appliance.

a After replacing the local site certificate, to re-establish the trust log in to the appliance management interface of the remote site.

b In the left pane, click **Settings**.

c Under **Site settings** next to **Pairing**, click **Repair**.

d To re-establish the trust with the site that has a replaced certificate, in the **Update Pairing** window confirm the Service Endpoint.

Option	Description
Service Endpoint	■ Enter the address of the Service Endpoint:443 of the remote VMware Cloud Director Availability appliance. ■ Alternatively, enter port 8048 when both VMware Cloud Director Availability appliances reside in the same network.
Description	Optionally, enter a description for this vSphere site as an identifier.

Verify the thumbprint and accept the SSL certificate of the Service Endpoint in the remote vCenter Server site.

e To re-establish the trust after replacing the remote site certificate, log in to the local site appliance management interface and repeat this step.

Change the IP Address of the Appliance

By using the appliance management interface, change its IP address, then by using the Replicator Service management interface, update the traffic control settings then restart the appliance services. By returning to the appliance management interface, repair the local Replicator Service and update the Service Endpoint address. Finally, repair from the remote site by using the updated Service Endpoint address.

Note Applying any network changes can lead to temporary network outages. For example, the browser connectivity to the management interface is interrupted when being accessed through the network adapter that is being reconfigured.

This procedure applies to the following appliance roles:

- **VMware Cloud Director Availability On-Premises Appliance roles:**
  - On-Premises to Cloud Director Replication Appliance
  - On-Premises to Cloud vCenter Replication Appliance

and for the provider appliance:

- vCenter Replication Management Appliance

For information about changing the appliance address in a cloud site backed by VMware Cloud Director, see Network Settings Configuration.

Prerequisites

Verify that VMware Cloud Director Availability 4.4 is deployed in the vCenter Server site.

Procedure

1 Log in to the management interface of the VMware Cloud Director Availability 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 Change the appliance network adapter IP address.

   a In the left pane, click **Settings**.

   b Under **Appliance settings**, expand the **Network** section.

   You can see all the network adapters that are added to the appliance.

   c Next to the adapter name which needs changing the IP address, click **Edit**.

   d In the **Settings** window for the selected adapter, configure its network settings and click **Apply**.

Option	Description
IP Mode	Select **IPv4**, **IPv6**, or **Unconfigured** By selecting **Unconfigured**, you turn off this adapter and delete all its settings, including static routes. Use this cleanup procedure, in case there are configuration leftovers that are causing unexpected network behavior.
Type: **DHCP**	If you select DHCP to provide the network configuration, all manually configured network settings, such as DNS servers, search domains, static routes, and MTU size are removed.
Type: Static	Enter the static configuration. 1 In the **Address/Prefix** text box, enter a CIDR address - IP address, followed by a forward slash and a network mask or a prefix length. For example, enter **`10.20.30.41/21`**. 2 In the **Gateway** text box, enter a gateway that is in the same network as the provided IP address. For each IP mode, you can use only one default gateway. If you are configuring a second adapter in the same IP mode, you must not enter a default gateway. 3 In the **MTU (bytes)** text box, enter the maximum transmission unit size in bytes. The default is 1500 bytes.

   The updated IP address applies, showing a continuously spinning progress indicator until you go to the management interface by using the new IP address.

3 Log in to the management interface of the local Replicator Service by using the new IP address of the appliance.

   a In a Web browser, go to `https://Appliance-New-IP-Address:8043/ui/admin`.

   Cancel selecting certificates for login displayed by your browser.

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

   c Click **Login**.

4 Update the **Traffic Control** addresses then restart the services of the appliance.

   a In the left pane, click **Settings**.

   b Under **Appliance settings**, next to the **Traffic Control** section, click **Edit**.

   c In the **Traffic Control** window, select the new IP address of the network adapter.

Option	Description
Management Address	Select the new IP address for the network adapter.
NFC Address	Select the new IP address for the network adapter.
LWD Address	Select the new IP address for the network adapter.

   d In the left pane, click **System Health**.

   e On the **System health** page, to restart all the appliance services, click **Restart service**.

   The web interface logs out your browser session. After the services restart in a few minutes, the page reloads.

   Note This step completes changing the IP address of:

   - On-Premises to Cloud Director Replication Appliance is now configured with the new IP address.

   Complete the remaining steps only when configuring new IP address for one of the following appliance roles:

   - On-Premises to Cloud vCenter Replication Appliance
   - vCenter Replication Management Appliance

5 Log in back to the management interface of the VMware Cloud Director Availability appliance.

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

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

   a Click **Login**.

6 Repair the local auto-paired Replicator Service on the appliance by updating the Service Endpoint address then restart the appliance services.

   a In the left pane, click **Replicator Services**.

   b Select the local Replicator Service of the appliance and click **Repair**.

   c In the **Details for the Replicator Service** window, update the Service Endpoint address with the new IP address and click **Apply**.

Option	Description
Endpoint Address	Enter the **`new IP address`** for the Service Endpoint of this appliance.
Appliance Password	Enter the password for the appliance **root** user.
SSO Admin Username	Enter the vSphere **administrator** user name for the vCenter Server Lookup service that belongs to the **ADMINISTRATORS** group.
SSO Password	Enter the vSphere **administrator** password for the vCenter Server Lookup service.

   Verify the thumbprint and accept the SSL certificate. The updated endpoint address applies, showing a continuously spinning progress indicator. If you missed restarting the appliance services in the previous step, you must retry this step after restarting them or you see: `Generic network error occurred at the client side.`

   d In the left pane, click **System Health**.

   e On the **System health** page, verify that all connectivity statuses show green `OK`.

7 Update the Service Endpoint of the appliance with the new IP address.

   a In the left pane, click **Settings**.

   b Under **Service endpoints**, next to **Service Endpoint Address** click **Edit**.

   c In the **Service Endpoint address** window, enter the new IP address and click **Apply**.

8 Update the new Service Endpoint address in the paired remote site.

   If the Service Endpoint address changed before any initial pairing with a remote site, skip this step.

   a From the remote site, in the left pane click **Peer Sites**.

   b Select the site with updated Service Endpoint address and click **Repair**.

   c In the **Update Pairing** window, click **Update**.

   d Verify the thumbprint and accept the SSL certificate of the site.

   The remote paired site uses the new Service Endpoint address.

Results

The VMware Cloud Director Availability appliance now uses the new IP address.

Unregister the VMware Cloud Director Availability vSphere Client Plug-In

To remove the established connection between the VMware Cloud Director Availability appliance and the vCenter Server instance, you remove the vCenter Server Lookup service registration by using the appliance management interface.

Procedure

1. Log in to the management interface of the VMware Cloud Director Availability 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 **Settings**.
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** user credentials and click **Remove**.

   The vCenter Server Lookup service is unregistered from the appliance configuration. After you log out and log in to vCenter Server, you can see that the VMware Cloud Director Availability vSphere Client Plug-In is unregistered from the vCenter Server instance.

Results

The 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 this appliance again, after running the initial setup wizard. If this site is still paired with a cloud site, use the same vCenter Server Lookup service as in the configuration before the pairing.

Monitoring and Troubleshooting 4

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

Support Knowledge Base

For troubleshooting information from the knowledge base articles for VMware Cloud Director Availability, see the latest Cloud Director Availability KB articles in the *VMware Knowledge Base*.

This chapter includes the following topics:

Schedule Backup Archives

In the management interface of the appliance, create backup schedule for generating new backup archives of VMware Cloud Director Availability. Connect and authenticate to an external server using Secure File Transfer Protocol (SFTP) for scheduled uploads of the backup archives as files for future restore to that moment in time.

This procedure is applicable to any the following VMware Cloud Director Availability appliance roles:

- Cloud Director Replication Management Appliance
- Cloud Director Combined Appliance
- On-Premises to Cloud Director Replication Appliance
- vCenter Replication Management Appliance
- On-Premises to Cloud vCenter Replication Appliance

You schedule the backup generation of VMware Cloud Director Availability only by using the management interface of the appliance. The scheduled backup archives contain the following information from each appliance in the site:

- Configuration files
- Public certificate
- Keystore
- Database dump

In the backup archive, this information is stored as multiple `.enc` appliance backup files. When generating the backup, you provide a password that encrypts the `.enc` appliance backup files to preserve any sensitive information.

A backup file does not contain:

- The appliance **root** user password.
- Any previous backup archives.
- Any support bundles.
- The NTP time server configuration.
- Enable SSH state.
- The network configuration provided in the OVF wizard during appliance deployment.
- Static routes configured on appliances with multiple network interface cards (NICs).

Note After evacuating a datastore, all backups taken priorly cannot restore the replications. For information about datastore evacuation, see Evacuate the Replication Data from a Datastore.

Prerequisites

- Verify that VMware Cloud Director Availability 4.5 or later is installed for scheduling backup archives to an SFTP server.

  Alternatively, for information about backing up the appliances to their local internal storage, see Back Up All Appliances in the Cloud and for all the remaining appliance roles, see Back Up the Appliance.

- Verify that the SFTP server is available and is reachable from VMware Cloud Director Availability.
- Verify that before taking a backup, all VMware Cloud Director Availability services are operational. As exception, unreachable Replicator Service instances without incoming replications do not prevent generating a backup. The scheduled backup generation fails when any other of the services cannot be reached or is not operational.
- Verify that the `free disk space` value in the bottom of the **System health** page shows at least 40 % amount of free space for each of the VMware Cloud Director Availability appliances in the site. The scheduled backup generation fails when there is insufficient storage.

Procedure

1 Log in to the management interface of the VMware Cloud Director Availability 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 **Backup Archives**.
3 On the **Scheduled backup archives** page, click **Configure schedule**.
4 Complete the **Create Backup Schedule** wizard.
   a On the **Server location** page, enter the SFTP protocol prefix, the SFTP server address, the SFTP network port, and the destination folder of the SFTP server for uploading the backup archives to then click **Next**.

      For example, in the **Server location** text box enter ***sftp://FQDN-or-IP-address:port/destination_folder/subfolder***, where the */destination_ folder/subfolder* path is relative to the root `/` directory on the SFTP server.
   b On the **Server authentication** page, select the authentication method for the SFTP connection, enter the following details then click **Next**.
      - **Authenticate using server credentials**: enter **Backup server user name** and **Backup server password**, then to establish a connection click **Test connection**. Verify and accept the SSH server public key.
      - **Authenticate using public key**: enter **Backup server user name**, click **Click to copy public key** paste appending it to the `authorized_keys` file in the SSH server, then to establish a connection click **Test connection**. Verify and accept the SSH server public key.

c On the **Backup schedule** page, specify the time between two scheduled backups in **Backup interval**, ranging from minimum of 30 minutes to a maximum of 1 week then click **Next**.

d On the **Encrypt backup** page, enter a password to protect the contents of the backup archive then click **Finish**.

The password that you must enter must contain a minimum of eight characters and must consist of:

- At least one lowercase letter.
- At least one uppercase letter.
- At least one number.
- At least one special character, such as & # % .

The **Schedule configuration pane** shows:

- **SFTP server location**
- **Backup server user name**
- **Backup interval**

In the table you see a `Generate scheduled backup archive` task progressing.

5 (Optional) To modify the backup schedule, click **Edit schedule** then complete the **Edit Backup Schedule** wizard.

On the **Server location** page, selecting the **Untrust the old SFTP server** check box removes the established trust with the previously configured SFTP server. If using key-based authentication, copy the new public key and paste appending it to the `authorized_keys` file in the SFTP server.

This trust is listed on the **Settings** page, under **Security settings** by expanding the **Trusted SSH hosts** section where you can also optionally click **Copy** or **Regenerate** for the `SSH public key`, or optionally click **Add** and in the **Add SSH host** window enter **Host** and **Port** then verify and accept the SSH server public key.

Results

At the scheduled time, VMware Cloud Director Availability starts backing up then uploads the backup files directly to the SFTP server.

What to do next

You can later download one of the scheduled backup files directly from the SFTP server for restoring VMware Cloud Director Availability to that moment in time. For information about restoring from a backup archive, see Restore Appliances in the Cloud.

To delete backup files, delete them directly from the SFTP server. This action has no effect on the backup task in the user interface.

Verify the Uptime and the Local and the Remote Connectivity in the Cloud

As a **service provider**, check both the services and the appliance uptime, then ensure that the connectivity between all the local services in the cloud site and the paired remote sites is `OK` on the **System Health** page by validating the **Service status** and the **Tunnel connectivity**. `Connection offline` identifies local or remote services that are inaccessible.

On the **System Health** page, verify the service uptime and the connectivity in the local cloud site.

Service uptime

Since VMware Cloud Director Availability 4.5, verify the time elapsed since the services and the appliance started.

- **Service uptime** shows the time that elapsed since all services on the appliance started.
- **Appliance uptime** shows the time that elapsed since the appliance started.

Service status

Verify the connectivity statuses in the local cloud site to the following infrastructure services.

- Connectivity to the vCenter Server Lookup service.
- Connectivity to the database of VMware Cloud Director Availability.
- Connectivity to VMware Cloud Director.
- Connectivity to the local Tunnel Service.
- Connectivity to the NTP server.

Tunnel connectivity

The following three sections are available for VMware Cloud Director Availability 4.3 and later for verifying the statuses of the connections from the local Tunnel Service to the following destinations.

- **Local components connectivity** to all the remaining VMware Cloud Director Availability services on the cloud appliances in the local cloud site.
- **Remote cloud sites connectivity** to the remote Tunnel Service instances in all paired remote cloud sites with the local cloud site.
- **On-Prem Incoming connectivity** to all paired On-Premises to Cloud Director Replication Appliance instances with the local cloud site.

Successful connectivity shows a green check icon `OK`. Alternatively, a red exclamation icon shows for connections that the Tunnel Service cannot establish. Restoring such connections automatically updates their connectivity status to green check icons `OK`.

Prerequisites

Verify that VMware Cloud Director Availability 4.5 or later is deployed for displaying the service uptime.

Procedure

1. Log in to the management interface of the VMware Cloud Director Availability 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 **System Health**.
3. To verify the elapsed time since the services started and the elapsed time since the appliance started, check both sections.
   - **Service uptime**
   - **Appliance uptime**
4. For the local connectivity in the cloud site with the infrastructure services like vCenter Server Lookup service, VMware Cloud Director, the NTP server, and others, under **Service status** verify that the connectivity reports a green check icon.
5. To verify the local connectivity in the cloud site, under **Tunnel connectivity** expand the **Local components connectivity** section.

   This section shows whether the local Tunnel Service successfully connects to the remaining services on the cloud appliances in the local cloud site. If any, the section also shows a red exclamation icon with a number of connections offline.

   All the local services to which the local Tunnel Service successfully establishes a connection show a green check icon `OK`. Alternatively, a service to which the local Tunnel Service cannot connect shows a red exclamation icon.

   If the local Tunnel Service is not operational, the entire **Local components connectivity** sections shows a red exclamation icon `Connection refused`. Also, under **Service status** the **Tunnel Service connectivity** shows a red exclamation icon `Connection refused`.
6. To verify the remote connectivity from the local cloud site to the paired remote cloud sites, under **Tunnel connectivity** expand the **Remote cloud sites connectivity** section.

   This section shows whether the local Tunnel Service successfully connects to each remote Tunnel Service in each paired remote cloud site. If any, the section also shows a red exclamation icon with a number of connections offline.

All the remote Tunnel Service instances in paired remote cloud sites to which the local Tunnel Service successfully establishes a connection show a green check icon `OK`. Alternatively, a remote Tunnel Service to which the local Tunnel Service cannot connect shows a red exclamation icon.

7 To verify the remote connectivity from the local cloud site to the paired on-premises sites, under **Tunnel connectivity** expand the **On-Prem Incoming connectivity** section.

The **On-Prem Incoming connectivity** section shows whether the local Tunnel Service successfully connects to each remote On-Premises to Cloud Director Replication Appliance in each paired on-premises site. If any, the section also shows a red exclamation icon with a number of connections offline.

All the remote On-Premises to Cloud Director Replication Appliance instances in paired on-premises sites to which the local Tunnel Service successfully establishes a connection show a green check icon `OK`. Alternatively, a remote On-Premises to Cloud Director Replication Appliance to which the local Tunnel Service cannot connect shows a red exclamation icon.

Results

You validated that the local cloud site connectivity is `OK`.

- For the infrastructure services in the local cloud site.
- For each VMware Cloud Director Availability service in the local cloud site.
- For all the paired remote sites, both cloud sites and on-premises sites.

Restart the VMware Cloud Director Availability Services

As part of the troubleshooting, you can restart all VMware Cloud Director Availability services in the appliance from the **System health** page.

Note 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 each VMware Cloud Director Availability 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 all of the appliance services.

a In the left pane, click **System Health**.

b In the **System health** page, click **Restart service**.

c In the **Restart service** window, to confirm the restart operation click **Restart**.

Collect Support Bundles

For troubleshooting purposes, VMware Technical Support might request support bundles that contain product-specific logs, configuration files, and data appropriate to the situation. You can collect the diagnostic information in a support bundle by using a specific management interface or a script.

Procedure

- Collect a support bundle for each VMware Cloud Director Availability appliance by using its service management interface.
  a. In a Web browser, go to the management interface of any of the VMware Cloud Director Availability appliances.

     To generate a complete support bundle from a cloud site backed by VMware Cloud Director, go to the management interface of the Cloud Director Replication Management Appliance.

Deployment type	Component	Management Interface
■ On-Premises to Cloud Director Replication Appliance ■ On-Premises to Cloud vCenter Replication Appliance ■ vCenter Replication Management Appliance	On-Premises	`https://Appliance-IP-Address/ui/admin`
Cloud Director Replication Management Appliance	Cloud Service	`https://Replication-Management-Appliance-IP-Address/ui/admin`
Replicator Appliance	Replicator Service	`https://Replicator-Appliance-IP-Address/ui/admin`
Tunnel Appliance	Tunnel Service	`https://Tunnel-Appliance-IP-Address/ui/admin`
Cloud Director Combined Appliance	Cloud Service	`https://Appliance-IP-Address/ui/admin`
	Manager Service	`https://Appliance-IP-Address:8441/ui/admin`
	Replicator Service	`https://Appliance-IP-Address:8440/ui/admin`
	Tunnel Service	`https://Appliance-IP-Address:8442/ui/admin`

  b. Log in as the **root** user.

  c. In the left pane, click **Support Bundles**.

d In the **Support bundles** page, click **Generate new**.

e In the **Generate a support bundle** window, to initiate creating a support bundle, click **Generate**.

The cloud site provider can also collect on-premises support bundles by activating the **Generate a support bundle from On-Premises site(s)** toggle. Then select the on-premises sites to include in the support bundle. The logs of all the selected on-premises appliances that allow* log collection from the cloud are included in the `cloud-bundle-id-date-timestamp.tar.bz2` file, under `manager/mgr.tar.bz2/onprems/rtr-id.tar.bz2`.

*Collecting on-premises logs from the cloud requires version 4.4 or later in both the cloud site and in the on-premises sites and also requires the on-premises administrator to activate the **Allow log collection from Cloud** toggle when initially pairing with the cloud site or during repairing. For information about allowing on-premises log collection from the cloud, see Repair a Site.

f After generating support bundles, in the **Bundle Id** column, to download a support bundle click the ***bundle id*** link.

g In the **Download Support Bundle** window, to save the support bundle file locally click **Download**.

In the Web browser, the `cloud-bundle-id-date-timestamp.tar.bz2` file starts downloading.

h After generating 10 support bundles, to generate new bundle first remove some of the old bundles by selecting them and clicking **Delete**.

If you attempt to generate an 11th support bundle, after you click **Generate** a **Warning** window shows `Support bundle quota exceeded. Number of allowed bundles: 10, current bundle count: 10.`

- If you cannot access the management interface of the VMware Cloud Director Availability appliance, collect a support bundle by using a Secure Shell (SSH) client.

a Open an SSH connection to the VMware Cloud Director Availability virtual machine and log in by using the **root** user credentials.

b Create a folder for the support bundle.

```
mkdir /opt/vmware/h4/serviceType/support/$(uuidgen)
cd /opt/vmware/h4/serviceType
```

For *serviceType*, use one of the arguments: **`cloud`**, **`manager`**, **`replicator`**, or **`tunnel`**, according to the Component in the above table.

- For On-Premises to Cloud Director Replication Appliance use **`replicator`**.
- For On-Premises to Cloud vCenter Replication Appliance use **`manager`**.
- For vCenter Replication Management Appliance use **`manager`**.

c To generate the support bundle run the `/opt/vmware/h4/bin/support-bundle.py` script and provide arguments with the deployment type of the appliance and the output folder.

- In a dedicated appliance deployment type, open an SSH connection to each VMware Cloud Director Availability appliance and run the script

```
/opt/vmware/h4/bin/support-bundle.py serviceType $(ls -t /opt/vmware/h4/
serviceType/support/ | head -1)
```

- For the Cloud Service, the following example collects all logs.

```
/opt/vmware/h4/bin/support-bundle.py cloud $(ls -t /opt/vmware/h4/cloud/support/ |
head -1)
```

d Download the `/opt/vmware/h4/serviceType/support/UUID/bundle-YYYY-MM-DD_HH-mm-SS-Time-Zone/serviceType-bundle-YYYY-MM-DD_HH-mm-SS-Time-Zone.tar.bz2` support bundle file.

- Collect a vCenter Server instance support bundle.

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 of the vCenter Server support bundle.

- For cloud sites backed by VMware Cloud Director, collect a VMware Cloud Director support bundle by using a Secure Shell (SSH) client.

a Open an SSH connection to the VMware Cloud Director 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 the `/opt/vmware/vcloud-director/data/transfer/vmware-vcd-support` folder.

Results

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

Record Your Screen with the Live Incident Assistant

In your web browser, to assist with live incident reporting you can record a selectable area of your screen and optionally, the microphone and the browser log directly by using VMware Cloud Director Availability.

The recording contains an encoded video file with your mouse movements, text entries, and all actions performed in the selected screen area, and optionally sound from your microphone.

In addition to the video file, when recording the VMware Cloud Director Availability window, the recording can also optionally contain a browser log file with VMware Cloud Director Availability entries only, with the passwords and the sensitive information censored.

Prerequisites

Verify that VMware Cloud Director Availability 4.2 or later is successfully deployed.

Procedure

1. Log in to the management interface of VMware Cloud Director Availability.
2. Before using the recording options, access the new recording icons.
   - Depending on the login method, if the top pane of VMware Cloud Director Availability is visible, next to the refresh button and the light/dark theme selector menu, there is a new recording icon.
   - Alternatively, on the **Dashboard** page next to **Topology**, click the **Report Issue** link.
   - Alternatively, to show or hide the new recording icon in the right pane on any VMware Cloud Director Availability page, press Ctrl + Shift + A.
3. To start the recording, click either of the new recording icons.
   a. In the **Before you continue** window, acknowledge the sensitive information message and click **Continue**.
   b. In the **Live Incident Assistant** window, select at least one recording option and click **Start**.

Option	Description
Capture video	Select to record a motion video track of the selected screen area. The resulting archive contains a `video.mp4` file with the video track.
Video quality	Select either **Low**, **Medium**, or **High** video encryption quality for the video track.
Capture audio	Select to record the audio track from your microphone. ■ If recording both audio and video, the resulting archive contains a `video.mp4` file with the video and the audio tracks. ■ If recording audio without **Capture video** selected, the resulting archive contains an `audio.webm` file with the audio track.
Capture browser logs	Select to record a censored text log with all web browser requests and responses between the VMware Cloud Director Availability portal and the backend server. The resulting archive contains a `browser-console.log` file.

c If you selected **Capture video**, accept your browser request for permission to capture your screen and select a screen recording area.

Depending on your web browser, you can select to share the following area with VMware Cloud Director Availability for recording:

- Your entire screen area, by selecting which monitor to record.
- A specific window, by selecting the application window for recording.
- A specific browser tab, by selecting the tab for recording.

If you cancel, block, or dismiss the screen sharing permissions without explicitly allowing them, an **Error** window shows a message that `Your browser denied the permissions required for capturing the screen. In the browser, select the screen capture area and allow the request from the appliance to share/see your screen after attempting another capture.`

d If you selected **Record audio**, accept your browser request for permission to use your microphone.

If you do not permit the audio sharing, an **Error** window shows a message that `Your OS blocks capturing your screen or your microphone. Allow the requested permissions to your browser before attempting another capture..`

4 Perform the actions that you want to be present in the recording.

The maximum session time is 30 minutes. If you do not stop the recording before they pass, you are prompted to download the recording or to discard it.

5 To stop the recording, in the place of the new recording icons, click either of the stop recording buttons or when recording video, you can click the stop sharing browser button.

Your browser downloads the `VCDA UI Support Bundle - hh_mm_ss.zip` file that contains the optional recorded motion video, the optional sound track, and the optional `browser-console.log` file.

What to do next

You can now send the recording archive for support.

Allow SSH Access

By default, VMware Cloud Director Availability does not allow Secure Shell (SSH) access. To connect to the VMware Cloud Director Availability appliance by using an SSH client, first you must allow the SSH access by using the management interface of the appliance.

Prerequisites

Verify that VMware Cloud Director Availability is successfully deployed in the site.

Procedure

1. Log in to the management interface of the VMware Cloud Director Availability 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 **Settings**.
3. Under **Security settings** next to **Allow SSH access**, click **Edit**.
4. In the **Allow SSH access** window, select **Allow SSH access** and click **Apply**.

Results

This VMware Cloud Director Availability appliance now allows SSH connections.

What to do next

You can connect to the VMware Cloud Director Availability appliance by using an SSH client and authenticating as the **root** user.

Configure Additional Service Logging Level

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

After exhausting the existing logs, advanced troubleshooting might require an extra level of logging detail. To generate the additional level of logging data, configure each VMware Cloud Director Availability service.

Procedure

1. Log in to the management interface of the VMware Cloud Director Availability 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 **Settings**.
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 of the service persists until this service restarts.

6 Connect to the VMware Cloud Director 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 VMware Cloud Director Availability services log files. For information about each service log file, select your version and see VMware Cloud Director Availability Logs in the *Security Guide*.

Change the Password of the root User

For security reasons, you can change the **root** users passwords of the VMware Cloud Director Availability appliances.

Procedure

1 Log in to the management interface of the VMware Cloud Director Availability appliance.
   a In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
   b Select **Appliance login** enter the **root** user credentials.
   c Click **Login**.
2 In the left pane under **Configuration**, click **Settings**.
3 Under **Appliance settings**, next to **Root password** click **Change**.
4 In the **VMware Cloud Director Availability Appliance Password** window, change the **root** user password.
   a In the **Current Password** text box, you must enter the current password of the **root** user.
   b In the **New Password** text box, enter the new password for the **root** user.

      The password that you enter must be a secured password with a minimum of eight characters and it must consist of:

      • At least one lowercase letter.
      • At least one uppercase letter.
      • At least one number.
      • At least one special character, such as & # %.
   c In the **Confirm Password** text box, enter the same new password.
   d To confirm the password change, click **Apply**.

Results

You changed the password of the **root** user of the appliance.

What to do next

You can change the **root** users passwords of the remaining VMware Cloud Director Availability appliances.

Note VMware Cloud Director Availability does not store the **root** user password for services communications and operations.

No further actions are required after any of the VMware Cloud Director Availability appliances **root** users passwords changes:

- The **root** user password is used only for administrative logins to the appliance.
- Changing the **root** user password of the Cloud Director Replication Management Appliance in a cloud site does not affect the paired cloud sites and does not affect the paired on-premises sites.
- The Replicator Service instances paired with the Cloud Service continue operating normally after changing the **root** users passwords of the Replicator Appliance instances and the Cloud Director Replication Management Appliance.
- The Cloud Service only uses the Tunnel Appliance **root** user password to enable the Tunnel Service for the first time.
- Changing the **root** user password of the On-Premises to Cloud Director Replication Appliance does not affect the pairing with the cloud site.

Configure After Changing the vCenter SSO Credentials

After changing the vCenter Server single sign-on credentials used to register VMware Cloud Director Availability with the vCenter Server Lookup service, in VMware Cloud Director Availability repair the registration with the vCenter Server Lookup service with changed credentials.

After changing the vCenter Server single sign-on credentials, you can perform the following steps in any order.

Procedure

1. Repair the on-premises appliances that are paired with the vCenter Server Lookup service instance with the changed vCenter Server single sign-on credentials.
   a. Open a Web browser and go to `https://On-Premises-Appliance-IP-Address`.
   b. Select **Appliance login** and enter the **root** user credentials.
   c. Click **Login**.
   d. In the left pane, click **Settings**.
   e. Under **Site details**, next to **Pairing** click **Repair**.
   f. Complete the **Update Pairing** wizard, and in the **Lookup Service** page, enter the new vCenter Server single sign-on credentials.

Repeat this step to repair all on-premises appliances that are paired with the vCenter Server Lookup service instance with changed vCenter Server single sign-on credentials.

2 In the cloud site backed by VMware Cloud Director, repair all Replicator Service instances with the new vCenter Server single sign-on credentials.

   a Open a Web browser and go to the Manager Service management interface at `https://Appliance-IP-Address:8441/ui/admin`.

   b Select **Appliance login** and enter the **root** user credentials.

   c Click **Login**.

   d In the left pane, click **Replicator Services**.

   e Select each Replicator Service with a site name that matches the current local site name, and click **Repair**.

   f In the **Details for the Replicator Service** window, enter the appliance password, the new vCenter Server single sign-on credentials, and click **Apply**.

   The selected Replicator Service instance is configured with the new vCenter Server single sign-on credentials. Repeat repairing all remaining Replicator Service instances in the cloud site backed by VMware Cloud Director.

3 Repair all paired cloud sites.

   a Open a Web browser and go to the management interface at `https://Appliance-IP-Address/ui/admin`.

   b Select **Appliance login** and enter the **root** user credentials.

   c Click **Login**.

   d In the left pane under **Configuration**, click **Peer Sites**.

   e Select a remote cloud site and click **Repair**.

   f In the **Update Pairing** window, click **Update**.

   Repeat this step and repair all paired cloud sites.

Results

The new vCenter Server single sign-on credentials for the vCenter Server Lookup service are propagated after repairing all on-premises appliances, repairing all Replicator Service instances, and repairing all cloud sites.

Free Up VMware Cloud Director Availability Appliance Disk Space

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

After using advanced troubleshooting or if the disk space is low you can regularly clean up the appliance disk space .

Procedure

1 Clear the VMware Cloud Director Availability appliance service logs.

   a Connect to the VMware Cloud Director 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 VMware Cloud Director 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 VMware Cloud Director 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 For dedicated Replicator Appliance instances, remove the core dumps.

   a Connect to each 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 VMware Cloud Director 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.

Cannot Access the VMware Cloud Director Availability Tenant Portal Through VMware Cloud Director

You are unable to access the VMware Cloud Director Availability Tenant Portal through the VMware Cloud Director Service Provider Admin Portal and the VMware Cloud Director Tenant Portal.

Problem

- The `Availability` menu option is not available in the VMware Cloud Director Service Provider Admin Portal and the VMware Cloud Director Tenant Portal, or clicking it does not open the VMware Cloud Director Availability Tenant Portal.
- In the VMware Cloud Director Availability logs, you see an error message such as `Unable to register vCAV plugin in vCD`.

Cause

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

Solution

1. Log in to the VMware Cloud Director 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. Re-register the VMware Cloud Director Availability plug-in with VMware Cloud Director.
   a. In the left pane under **Configuration**, click **Settings**.
   b. Under **Service endpoints**, next to the **VMware Cloud Director address** click **Edit**.
   c. In the **VMware Cloud Director Details** window, configure the VMware Cloud Director endpoint.

Option	Description
VMware Cloud Director Endpoint address	Enter the endpoint address as `https://`*`VMware-Cloud-Director-IP-Address`*`:443/api`.
VMware Cloud Director Username	Enter the **system administrator** user name, that is used for all administrative operations. For example, *administrator@system*, where *system* is the name of the system organization of VMware Cloud Director.
VMware Cloud Director Password	Enter the **system administrator** password.

d Click **Apply**.

e To complete the VMware Cloud Director configuration, verify the thumbprint and accept the VMware Cloud Director SSL certificate.

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

Unregister the VMware Cloud Director Availability Plug-Ins from VMware Cloud Director

Before removing the VMware Cloud Director Availability appliances, or if you see multiple instances of the plug-ins in VMware Cloud Director, as a **service provider** you can remove the plug-ins.

The Cloud Service installs the plug-ins in VMware Cloud Director named `Setup DRaaS and Migration` and `Availability (localSite)` during the registration with VMware Cloud Director. For more information, see Configure a Cloud Service Instance.

As a **service provider**, you remove both plug-ins before removing the Cloud Director Replication Management Appliance, or if you see multiple instances of the plug-in.

Note If you removed the Cloud Director Replication Management Appliance before following this procedure, see Delete a Plug-in in the VMware Cloud Director documentation.

Prerequisites

Verify that VMware Cloud Director Availability is successfully deployed in the cloud site.

Procedure

1 Log in to the Cloud Service management interface.

a Open a Web browser and go to `https://Appliance-IP-Address/ui/admin`.

b Select **Appliance login** and enter the **root** user credentials.

c Click **Login**.

2 In the left pane under **Configuration**, click **Settings**.

3 Under **Service endpoints**, next to **VMware Cloud Director address** click **Remove plugin**.

4 In the **Remove VCD UI plugin** window, click **Remove**.

Results

The VMware Cloud Director Availability plug-ins are unregistered from VMware Cloud Director.

What to do next

You can remove the VMware Cloud Director Availability appliances.