VMware Cloud Director Availability Administration Guide

2 JUN 2020

VMware Cloud Director Availability 4.0

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

What Is VMware Cloud Director Availability and How Does It Work

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
- Native integration with VMware Cloud Director™ by using the VMware Cloud Director plug-in for the replication management
- Access for tenant and cloud provider users by using the VMware Cloud Director Availability Tenant Portal
- Access for tenant 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 VMware vSphere®

Replication and migration features provided by VMware Cloud Director Availability:

- Full onboarding and migration capabilities from a single administration interface

- Automated inventory collection of virtual data centers, unprotected and protected vApps and virtual machines, storage profiles, and network configuration
- Self-service virtual machine migration from on-premises resources to cloud, cloud to on-premises resources, or cloud to cloud vApp, and virtual machine migrations between VMware Cloud Director instances
- Managed onboarding and disaster recovery capabilities for on-premises resources to cloud, and cloud to cloud scenarios
- Automated tenant replication, migration, failover, and failback of vApps and operations after a failover

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

Service level agreement (SLA) provided by VMware Cloud Director Availability:

- 5 minutes 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 Cloud Replicator Appliance
- Built-in optional compression of the replication traffic

Day-2 cloud provider 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

Clustering support:

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

How Does VMware Cloud Director Availability Work

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

In an on-premises environment, Replicator Service and a preconfigured instance of Tunnel Service 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

2

After installing and configuring VMware Cloud Director Availability, as a **service provider** you can perform management and administrative tasks. These tasks include changes to the provisioned environment and routine administration and maintenance procedures.

This chapter includes the following topics:

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.

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 the VMware Cloud Director Availability 4.0 appliance 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, click **Configuration**.
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 the VMware Cloud Director Availability 4.0 appliance 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, click **Configuration**.

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 the VMware Cloud Director Availability 4.0 appliance 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, click **Configuration**.
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 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 **Configuration**.

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.

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 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
[]
```

Certificates Management

When the SSL certificates are about to expire, the service provider 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 Replication Management Appliance operating the Cloud Service and the Manager Service.
- Cloud Replicator Appliance operating the Replicator Service.
- Cloud 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 VMware Cloud Director Availability On-Premises 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 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, click **Configuration**.
3. Under **Appliance settings**, next to **Certificate** click **Regenerate**.
4. In the **Regenerate Certificate** window, click **Apply**.

Results

After the certificate is regenerated, all 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, click **Configuration**.
3. Under **Appliance settings**, next to **Certificate** click **Import**.
4. In the **Import Certificate** window, enter the certificate details and click **Apply**.
   a. Enter the password that protects the keystore and the certificate private key.
   b. Click **Browse** and select the PKCS#12 file.

Results

After you upload the CA-signed certificate, all 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. With the new certificate, reestablish the trust with the local Tunnel Service and re-pair all cloud sites.

Replacing the Cloud Service certificate invalidates the trust with both the local and the remote Tunnel Service instances and the paired cloud sites. Reestablish the trust with the local Tunnel Service and re-pair the cloud sites.

Procedure

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

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

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

   c Click **Login**.

2 Replace the certificate of the Cloud Service.

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

   b Under **Appliance settings** next to **Certificate**, select the certificate replacement method.

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

   c Click **Apply**.

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

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

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

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

   c Click **Login**.

4 Trust the new certificate of the Cloud Service in the Tunnel Service.

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

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

   c In the **Tunneling Settings** window, enter the Tunnel Service **root** user credentials and click **Apply**.

   d To complete the trust reestablishment, accept the local Tunnel Service SSL certificate.

5 Trust the new Cloud Service certificate in the paired cloud sites.

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

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

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

   d To complete the trust reestablishment, accept the remote Cloud Service SSL certificate.

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

What to do next

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

Replace the Manager Service Certificate

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

Replacing the certificate of the Manager Service invalidates the trust between all Replicator Service instances in the local site, remote cloud sites, and remote on-premises sites. To reestablish the trust, re-pair the registration of Replicator Service instances in the remote site and re-pair the cloud sites.

Important After re-pairing all the cloud sites, you must also manually re-pair all on-premises 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 Manager Service certificate.

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

   b Under **Appliance settings** next to **Certificate**, select the certificate replacement method.

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

   c Click **Apply**.

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

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 in the local Replicator Service.

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

   b On the **Replicators administration** page, select the local Replicator Service and click **Repair**.

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

   d To complete the trust reestablishment, accept the local Replicator Service SSL certificate.

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

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

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

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

   c Click **Login**.

6 Trust the new Manager Service certificate in the paired cloud sites.

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

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

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

   d To complete the trust reestablishment, accept the remote Cloud Service SSL certificate.

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

What to do next

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

Replace the 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.

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
Combined Appliance	`https://Appliance-IP-Address:8440/ui/admin`
Cloud Replicator Appliance	`https://Replicator-Appliance-IP-Address/ui/admin`

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

   b Click **Login**.

2 Log in as **root**.

3 Generate or upload a new certificate.

4 Re-pair the registration of 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
Combined Appliance	`https://Appliance-IP-Address:8442/ui/admin`
Cloud Tunnel Appliance	`https://Tunnel-Appliance-IP-Address/ui/admin`

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

   b Click **Login**.

2 Log in as **root**.

3 Generate or upload a new certificate.

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

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

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

   c Click **Login**.

5 In the left pane, click **Configuration** and next to **Tunnel address** click **Edit**.

6 In the **Tunneling settings** window, click **Apply**.

7 Verify the thumbprint and accept the new 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 trust the new certificate and communicate with VMware Cloud Director.

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

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, click **Configuration**.
3. Under **Service endpoints**, next to **Cloud Director address** click **Edit**.
4. On the **Cloud Director Details** page, click **Apply**.
5. Verify the thumbprint of the certificate, and click **Accept**.

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

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

Prerequisites

- Verify that the SSL certificate of the Platform Services Controller certificate is successfully renewed, and that the vCenter Server Lookup service is updated to use the renewed certificate. For information about replacing the SSL certificate on a Platform Services Controller, see VMware KB 2118939.

- Verify that all components in your environment that depend on the vCenter Server registration in the vCenter Server Lookup service are configured to trust the renewed certificate. An example of such a component is NSX Manager.

Procedure

1 Configure the Replicator Service to work with the renewed Platform Services Controller 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:8440/ui/admin`.

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

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

  d Under **Service endpoints**, next to **Lookup service address** click **Edit**.

  e In the **Lookup Service Details** dialog box, enter the vCenter Server Lookup service address and click **Apply**.

    The details of the renewed vCenter Server Lookup service certificate appear.

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

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

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

2 Configure the Manager Service to work with the renewed Platform Services Controller certificate.

  Repeat this step for all Manager Service instances.

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

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

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

  d Under **Service endpoints**, next to **Lookup service address** click **Edit**.

  e In the **Lookup Service Details** dialog box, enter the vCenter Server Lookup service address and click **Apply**.

    The details of the renewed 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 Monitoring**.

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

3 Configure the Cloud Service to work with the renewed Platform Services Controller certificate.

   Repeat this step for all Cloud Service instances.

   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, click **Configuration**.

   d Under **Service endpoints**, next to **Lookup service address** click **Edit**.

   e In the **Lookup Service Details** dialog box, enter the vCenter Server Lookup service address and click **Apply**.

      The details of the renewed vCenter Server Lookup service certificate appear.

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

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

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

4 If you are using a single sign-on login to Tunnel Service, configure the Tunnel Service to work with the renewed Platform Services Controller certificate.

   Repeat this step for all Tunnel Service instances.

   a In a Web browser, go to the Tunnel Service management interface at `https://Tunnel-Appliance-IP:8442/ui/admin`.

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

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

   d Under **Service endpoints**, next to **Lookup service address** click **Edit**.

   e In the **Lookup Service Details** dialog box, enter the vCenter Server Lookup service address and click **Apply**.

      The details of the renewed 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 Monitoring**.

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

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. Each VMware Cloud Director Availability instance allows the service provider to manage the accessible provider VDCs.

Procedure

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

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

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

   c Click **Login**.

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

3 Under **Site details**, next to **Accessible Provider VDCs**, click **Edit**.

4 In the **Accessible Provider VDCs** windows, select **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.

Managing Connections Between Cloud Sites

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

VMware Cloud Director Availability to VMware Cloud Director Availability Interoperability

You can pair sites that have different VMware Cloud Director Availability versions deployed. For example, you can pair a cloud site where version 4.0 is deployed with an on-premises site where version 3.5 is deployed. You can also pair with a cloud site where version 3.5 is deployed. This scenario can occur when upgrading the sites one at a time or to migrate workloads from an earlier vSphere and VMware Cloud Director versions to a site with current vSphere and VMware Cloud Director versions.

Note When pairing sites with different VMware Cloud Director Availability versions, only the functionality of the earlier version is supported. For example, only the functionality of version 3.5 is supported when pairing a site where version 3.5 is deployed with a site where version 4.0 is deployed.

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 the VMware Cloud Director Availability On-Premises Appliance and the Version of VMware Cloud Director Availability in the Cloud Site

VMware Cloud Director Availability On-Premises Appliance	Cloud Site 3.0	Cloud Site 3.5	Cloud Site 4.0
3.0	Supported	Supported	Supported
3.5	Supported	Supported	Supported
4.0	Supported	Supported	Supported

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

Source Cloud Site VMware Cloud Director Availability	Destination Cloud Site 3.0	Destination Cloud Site 3.5	Destination Cloud Site 4.0
3.0	Supported	Supported	Supported
3.5	Supported	Supported	Supported
4.0	Supported	Supported	Supported

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

For example:

- 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.

Migration from Earlier VMware Cloud Director Availability Versions

By pairing an earlier and the latest VMware Cloud Director Availability versions, you can migrate workloads from source sites where the latest 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 the latest vSphere and VMware Cloud Director versions. For example, see the following table:

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

Source Site VMware Cloud Director Availability	Destination Site VMware Cloud Director Availability
On-premises site A, deployed version 3.5 with vSphere 5.5 or later.	Cloud site B, VMware Cloud Director Availability 4.0 with a supported VMware Cloud Director version*.
Cloud site X, deployed version 3.0 with vCloud Director 8.2, 9.0 or 9.1.	
Cloud site Y, deployed version 3.5 with vCloud Director 9.0 or 9.1.	

- 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 4.0 deployed in a cloud site with a supported VMware Cloud Director version*. You can then migrate all virtual machines to the later cloud site.
- 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.

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 bellow.

Before deploying VMware Cloud Director Availability On-Premises Appliance, verify the supported versions of vCenter Server, ESXi, and NSX by following the link bellow.

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

Pair Cloud Sites

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

Depending on the VMware Cloud Director Availability version in the cloud sites, use the appropriate pairing process:

- To pair site A and site B, both running version 3.5 or newer, perform the following pairing procedure from both sites:
  a From site A, initiate the pairing process with site B.
  b From site B, complete the pairing process with site A.

- To pair a site X running version 3.5 or newer and a site Y running version 3.0.x, perform the following steps:
  a In the X site, allow the administrative access from public IPs. For more information, see Allow Public Administrative Access to VMware Cloud Director Availability.
  b In the Y site, initiate and complete the pairing process with the X site.
  When pairing from the Y site, you must provide the password of the **root** user. For more information, see Pair 3.0.x Cloud Sites.
  c In the X site, after completing the pairing process, restrict the administrative access from public IPs. For more information, see Restrict Public Administrative Access to VMware Cloud Director Availability.
- To pair sites, both running version 3.0.x, see Pair 3.0.x Cloud Sites.

Prerequisites

Verify that all the VMware Cloud Director Availability appliances are configured in both cloud sites:

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

Procedure

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

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

5 To complete the first half of the pair process, verify the thumbprint and accept the remote Cloud Service SSL certificate.

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

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

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

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

What to do next

You can configure new replications, after modifying the default replication policy for both the source and for the destination organization to allow replications. Alternatively, a custom replication policy that is assigned to the source and to the destination organizations must allow replications. For information about the replication policy, see Configuring Replication Policies in *VMware Cloud Director Availability User Guide*.

Re-Pair Cloud Sites

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.

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

- To re-pair site A and site B, both running version 3.5 or newer, perform the following re-pairing procedure from both sites:
  a From site A, initiate the re-pairing process with site B.
  b From site B, to complete the re-pairing process, re-pair with site A.
- To re-pair a site X running version 3.5 and a site Y running version 3.0.x, perform the following steps:
  a In the X site, allow the administrative access from public IPs. For more information, see Allow Public Administrative Access to VMware Cloud Director Availability.
  b In the Y site, initiate and complete the re-pairing process with the X site.

    When pairing from the Y site, you must provide the password of the **root** user. For more information, see Re-Pair 3.0.x Cloud Sites .
  c In the X site, restrict the administrative access from public IPs. For more information, see Restrict Public Administrative Access to VMware Cloud Director Availability.
- To re-pair sites, both running version 3.0.x, see Re-Pair 3.0.x Cloud Sites .

Procedure

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

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

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

   c Click **Login**.

2 In the left pane, click **Sites**.

3 On the **Cloud sites** page, click **Repair**.

4 In the **Update Pairing** window, configure the connection to the cloud site and click **Update**.

Option	Description
Service Endpoint	Verify that the displayed IP address and port of the Cloud Tunnel Appliance in the remote site is correct.
Description	Optionally provide a description for the cloud site pair.

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

   The trust between the two sites is successfully reestablished.

6 On the **Cloud sites** page, verify that the site is listed as `Repaired`.

Results

You reestablished the cloud sites 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 *VMware Cloud Director Availability User Guide*.

Unpair Paired Sites

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

Prerequisites

Delete all configured replications with the paired site.

Procedure

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

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

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

   c Click **Login**.

2 In the left pane, click **Sites**.

3 Remove the established trust with a cloud site.

   a On the **Cloud sites** page, click **Delete**.

   b To remove the cloud site pairing, in the **Delete Peer Cloud Site** window, 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 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 To remove the on-premises site pairing, in the **Delete Peer Cloud Site** window, click **Delete**.

   You removed the cloud site trust with the on-premises site and you see a `Peer site 'on-prem-site-name' was not found` message. 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 Cloud Site from On-Premises.

Managing Public Administrative Access to VMware Cloud Director Availability

In a dedicated appliance deployment type, the administrative sessions to all VMware Cloud Director Availability services are restricted by default when originating from public networks.

The restriction applies to the following administrative accounts:

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

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

Allow Public Administrative Access to 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 Replication Management Appliance.

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

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

   c Click **Login**.

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

3 Under **Security settings**, next to **Restrict Admin APIs by source IP**, click **Edit**.

4 In the **Restrict Admin APIs by source IP** window, select **Allow admin access from anywhere** and click **Apply**.

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

Results

The external administrative sessions to all 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 Replication Management Appliance.
   a. In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
   b. Select **Appliance login** or **SSO login** and enter the **root** or the ***single sign-on*** user credentials.
   c. Click **Login**.
2. In the left pane, click **Configuration**.
3. Under **Security settings**, next to **Restrict Admin APIs by source IP** click **Edit**.
4. In the **Restrict Admin APIs by source IP** window, select **Do not allow admin sessions from the Internet (recommended)** and click **Apply**.

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

Results

The administrative sessions from public IPs to all VMware Cloud Director Availability services are restricted.

Maintenance

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

Evacuate the Replication Data from a Datastore

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

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

Prerequisites

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

Procedure

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

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

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

   c Click **Login**.

2 In the left pane, click **Datastores**.

3 To see a filter showing the replications that are placed on the highlighted datastore, click **Preview**.

4 Select a local datastore that lists a replications counter and click **Evacuate**.

5 In the **Evacuate datastore** window, select the destination storage policy for all incoming replications residing on the datastore and click **Apply**.

   - **Reset current storage policy** apply the current storage policy to each matching replication. After removing or adding datastores to the storage policy, this option can move the replication replica files, to make the matching replications compliant with their storage policy.
   - **Any** store all the replications to all the shared datastores to which the `Any` storage policy is applied.
   - ***pVDC Storage policy*** apply the selected storage policy to all matching replications. If the *pVDC Storage policy* is not exposed to a tenant data center, the replications of this tenant remain placed on the datastore.

Results

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.

Cloud Event Notifications

As a **service provider**, you can monitor the cloud event notifications that VMware Cloud Director Availability generates either by using a syslog server or in VMware Cloud Director by monitoring the VMware Cloud Director Availability events.

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

- **Syslog events**

  You can use the syslog protocol to forward the events to a preconfigured syslog server, for example vRealize Log Insight. By default, the syslog events are disabled. To configure them, see Forward Cloud Event Notifications.

- **VMware Cloud Director events**

  In VMware Cloud Director portal, 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. By default, the VMware Cloud Director events are enabled.

  Both delivery channels carry the same notification information, that is formatted according to the delivery method. You can use both **VMware Cloud Director events** and **Syslog events** at the same time, use either of them, or not use cloud event notifications.

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

  On-demand events

  User actions generate these events, for example, starting a replication, replication operations, policy changes, and others.

  User-initiated events

  The system generates these events, for example, periodic checks that are generated when a certain criteria is met.

Table 2-4. On-Demand 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

Table 2-4. On-Demand Events (continued)

Event Type	Log Level	Resource ID	Description	Details
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
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

Table 2-5. User-Initiated 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
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

Table 2-5. User-Initiated Events (continued)

Event Type	Log Level	Resource ID	Description	Details
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
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

Table 2-5. User-Initiated Events (continued)

Event Type	Log Level	Resource ID	Description	Details
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

Forward Cloud Event Notifications

As a **service provider**, you can forward the VMware Cloud Director Availability cloud event notifications to a syslog server and to VMware Cloud Director. Both delivery channels carry the same event information.

You can forward VMware Cloud Director Availability events to a syslog server and to VMware Cloud Director. You can use each delivery channel, both at the same time, or neither of them.

Prerequisites

Verify that VMware Cloud Director Availability 4.0 is deployed in the cloud site.

Procedure

1. Log in to the management interface of the Cloud 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, click **Configuration**.
3. Under **Notification settings** next to **Cloud event notifications**, click **Edit**.
4. In the **Cloud event notifications** window, configure the event settings.

Option	Description
Config poll interval	Time interval between polls for configuration issues. The default value is 1 day.
Connectivity poll interval	Time interval between polls for connectivity issues. The default value is 30 sec.
Replications poll interval	Time interval between polls for replication issues. The default value is 5 min.
Certificate expiry threshold	The time before a certificate expires to start forwarding events. The default value is 30 days.
RPO violation threshold	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 min.

Option	Description
RPO violation threshold	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.
Event reposting time	Time before a given event is forwarded again, while the condition is still active. The default value is 86400 sec (24 h).

5 To forward the events to the syslog server, enable **Syslog events**, and in the **Syslog server address and port** text box, enter the syslog server address and the UDP port.

6 To forward the cloud event notifications to VMware Cloud Director, enable **VMware Cloud Director events**.

7 To save the cloud event notifications configuration, click **Apply**.

Results

VMware Cloud Director Availability starts forwarding cloud event notifications to the selected destinations.

What to do next

You can monitor VMware Cloud Director Availability by using the syslog server or VMware Cloud Director.

Troubleshooting

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

Configure After Changing the vCenter Single Sign-On Credentials

After changing the vCenter Single Sign-On credentials used to register VMware Cloud Director Availability with the vCenter Server Lookup service, repair the Manager Service with all local instances of the Replicator Service. You must repair all VMware Cloud Director Availability On-Premises Appliance instances paired with the vCenter Server Lookup service instance with changed vCenter Single Sign-On credentials. You must also repair all paired cloud sites.

After changing the vCenter Single Sign-On credentials in vCenter Server, you can perform the following steps in any order.

Procedure

1 Repair the Replicator Service instances with the new vCenter 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 Single Sign-On credentials, and click **Apply**.

The selected Replicator Service instance is configured with the new vCenter Single Sign-On credentials. Repeat repairing all remaining Replicator Service instances in the cloud site.

2 (Optional) Repair the VMware Cloud Director Availability On-Premises Appliance instances that are paired with the vCenter Server Lookup service instance with the changed vCenter 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 **Configuration**.

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 Single Sign-On credentials.

Repeat this step to repair all VMware Cloud Director Availability On-Premises Appliance instances that are paired with the vCenter Server Lookup service instance which vCenter Single Sign-On credentials changed.

3 Repair all paired cloud sites.

a Open a Web browser and go to the Cloud Service 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, click **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 Single Sign-On credentials for the vCenter Server Lookup service are propagated after repairing all Replicator Service instances, repairing all VMware Cloud Director Availability On-Premises Appliance instances, and repairing all cloud sites.

Restore a Cloud Tunnel Appliance

To restore a failing Cloud Tunnel Appliance, you can power it off and deploy a new instance of the appliance.

Prerequisites

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

Procedure

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

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

   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 Cloud 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability On-Premises 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 VMware Cloud Director Availability Operational Verification.

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 Replication Management Appliance, or if you see multiple instances of the plug-in.

Note If you removed the Cloud 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, click **Configuration**.
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.

VMware Cloud Director Availability Operational Verification

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

Prerequisites

Verify that VMware Cloud Director Availability is successfully deployed and powered on.

Procedure

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

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

   b Log in as the **root** user.
   c In the left pane, click **System Monitoring**.
   d In the **Service status** section, verify that all connectivity checks report a green check icon.
4 Verify that the Tunnel Service instances are operational.
   a Open a Web browser and go to the management endpoint for your deployment type.

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

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

Results

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

What to do next

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

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

Restart the VMware Cloud Director Availability Services

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

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

Procedure

1. Log in to the management interface of the Cloud Replication Management Appliance.
   a. In a Web browser, go to `https://`*`Appliance_IP_Address`*`/ui/admin`.
   b. Select **Appliance login** or **SSO login** and enter the **root** or the ***single sign-on*** user credentials.
   c. Click **Login**.
2. Restart the Cloud Service and the Manager Service.
   a. In the left pane, click **System Monitoring**.
   b. Under **System health**, click **Restart service**.
   c. In the **Restart service** window, confirm the restart operation by clicking **Restart**.

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

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

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

   b Click **Login**.

4 Restart the Replicator Service.

   a In the left pane, click **System Monitoring**.

   b Under **System health**, click **Restart service**.

   c In the **Restart service** window, confirm the service restart by clicking **Restart**.

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

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

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

   b Click **Login**.

6 Restart the Tunnel Service.

   a In the left pane, click **System Monitoring**.

   b Under **System health**, click **Restart service**.

   c In the **Restart service** window, confirm the service restart by clicking **Restart**.

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 Tenant Portal.

   a Open a Web browser and go to `https://Cloud-Manager-IP-address/ui/admin`.

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

2 Re-register the VMware Cloud Director Availability plug-in with VMware Cloud Director.

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

   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.

Allow SSH Access

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

Prerequisites

Verify that VMware Cloud Director Availability is successfully deployed in the site.

Procedure

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

Results

The 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.

How Do You Collect Support Bundles

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

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

Procedure

1 Collect a support bundle for the VMware Cloud Director Availability components by using the service management interface.

a In a Web browser, go to the management interface for each VMware Cloud Director Availability component.

Deployment type	Component	Management Interface
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`
Cloud Replicator Appliance	Replicator Service	`https://`*`Replicator-Appliance-IP-Address`*`/ui/admin`
Cloud Tunnel Appliance	Tunnel Service	`https://`*`Tunnel-Appliance-IP-Address`*`/ui/admin`

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

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

d On the **Support bundles** page, click **Generate new**.

e In the **Bundle generate** window, initiate the creation of a support bundle by clicking **Generate**.

f After the support bundle is generated, in the **Bundle Id** column, initiate a download by clicking the ***bundle id*** link.

g In the **Download Support Bundle** window, save the support bundle file locally by clicking **Download**.

h After your browser downloads the file, optionally select the bundle and click **Delete**.

2 If you cannot access the VMware Cloud Director Availability service management interface, 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.

```
cd /opt/vmware/h4/serviceType
mkdir bundles
```

For *serviceType* use one of the arguments: **`cloud`**, **`manager`**, **`replicator`**, or **`tunnel`**.

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

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

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

- In a dedicated appliance deployment type, open an SSH connection to each VMware Cloud Director Availability appliance and run the script

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

For *serviceType* use one of the arguments: **`cloud`**, **`manager`**, **`replicator`**, or **`tunnel`**.

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

3 Collect a 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 `/opt/vmware/vcloud-director/data/transfer/vmware-vcd-support`.

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

a In a Web browser, go to `https://`*`vCenter-Server-FQDN`*`:443/appliance/support-bundle`.

b Log in by using the **root** user credentials, and click **Enter** to start the download.

Results

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

How Do You Set Additional Logging Level

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

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

Procedure

1. Log in to the management interface of the Cloud Replication Management Appliance.
   a. In a Web browser, go to `https://Appliance-IP-Address/ui/admin`.
   b. Select **Appliance login** or **SSO login** and enter the **root** or the ***single sign-on*** user credentials.
   c. Click **Login**.
2. In the left pane, click **Configuration**.
3. Under **Appliance settings** next to **Logging levels**, click **Edit**.
4. In the **Edit Log Levels** window, for each service you can set the logging level from **Off** to **All**.
5. To apply the configuration, click **Apply**.

   The modified logging level persists until the service restarts.
6. Connect to the 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.

VMware Cloud Director Availability Service	Service Log File Location
Manager Service	`/opt/vmware/h4/manager/log/manager.log`
Replicator Service	`/opt/vmware/h4/replicator/log/replicator.log`
Cloud Service	`/opt/vmware/h4/cloud/log/cloud.log`
Tunnel Service	`/opt/vmware/h4/tunnel/log/tunnel.log`

How Do You Free Up VMware Cloud Director Availability Appliance Disk Space

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

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

Procedure

1 Clear the 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 If you have a dedicated Cloud Replicator appliance, remove the core dumps.

   a Connect to the Cloud Replicator appliance by using a Secure Shell (SSH) client and authenticate as the **root** user.

   b Navigate to the `/var/core/` folder and remove the HBR `core*` files.

Results

The available disk space on the 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.

Administration On-Premises

3

After installing and configuring the VMware Cloud Director Availability On-Premises Appliance, you can re-pair or unpair the cloud sites from the on-premises site and unregister the VMware Cloud Director Availability On-Premises Appliance from vCenter Server.

This chapter includes the following topics:

Re-Pair On-Premises with Cloud Site

To reestablish the trust between the on-premises site and a cloud site, you re-pair the cloud site from the VMware Cloud Director Availability On-Premises Appliance.

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-Prem-Appliance-IP-address/ui/admin`.
   b. Log in as the **root** user.
2. In the left pane, click **Configuration**.
3. Under **Site details**, next to **Pairing** click **Repair**.
4. To re-establish the trust with the cloud site complete the **Update Pairing** wizard.
   a. On the **Site Details** page, verify the site name and description and click **Next**.
   b. On the **Lookup Service Details** page, enter the **`single sign-on`** user credentials and click **Next**.

c On the **Cloud Service Details** page, provide the **organization administrator** credentials and configure access from cloud.

Option	Description
Service Endpoint address	VMware Cloud Director Availability Service Endpoint:8048
Organization Admin	VMware Cloud Director ***admin@org***
Organization Password	VMware Cloud Director ***organization admin password***
Allow Access from Cloud	Select to allow the cloud provider and the organization administrators to perform the following operations from the VMware Cloud Director Availability Tenant Portal without authenticating to the on-premises site: ■ Discover on-premises workloads and replicate them to the cloud. ■ Reverse existing replications to the on-premises site. ■ Replicate cloud workloads to the on-premises site. Deselect to only allow users authenticated to the on-premises VMware Cloud Director Availability Tenant Portal to configure new replications and existing replications cannot be reversed from the VMware Cloud Director Availability Tenant Portal.

d Verify the thumbprint and accept the SSL certificate of the VMware Cloud Director Availability Service Endpoint.

e On the **Ready to complete** page, optionally select to configure the local placement, and to complete the initial setup wizard click **Finish**.

- You can configure data center to cloud replications and you can leave **Edit / configure local placement now** deselected.
- To enable the cloud to data center replications, select **Edit / configure local placement now**.

5 Verify that the connectivity to the cloud site is operational.

a In the left pane, click **System Monitoring**.

b Under **Cloud Service Status**, verify that for the cloud site you re-paired, **Service connectivity** shows a green OK status.

Results

The pairing between the on-premises site and the cloud site is re-established. If you did not configure local placement for the VMware Cloud Director Availability On-Premises Appliance, see Configure Local Placement in the *VMware Cloud Director Availability Administration Guide* document.

Unpair Cloud Site from On-Premises

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

Prerequisites

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

Procedure

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

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

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

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

3 Remove the established trust with the cloud site from the on-premises site.

   If from the cloud site the on-premises site is already unpaired, delete the remaining record in the on-premises site.

   a Under **Site details**, next to **Pairing** click **Unpair**.

   b In the **Unpair from cloud site** window, enter the VMware Cloud Director organization **administrator** credentials and click **Apply**.

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

Results

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

What to do next

- If you performed this procedure from the on-premises site first, in the cloud site 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.
- 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 pair the on-premises appliance and the cloud Replicator Service again, from the on-premises site, see Re-Pair On-Premises with Cloud Site.

Unregister the VMware Cloud Director Availability vSphere Client Plug-In

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

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-Prem-Appliance-IP-address/ui/admin`.
   b. Log in as the **root** user.
2. In the left pane, click **Configuration**.
3. Under **Service endpoints**, next to **Lookup Service Address** click **Remove**.
4. In the **Remove Lookup Service Registration** window, enter the single sign-on **administrator** credentials and click **Remove**.

   The vCenter Server Lookup service is unregistered from the VMware Cloud Director Availability On-Premises 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 on-premises vCenter Server.

Results

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

What to do next

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