Upgrade HCMF

Before You Upgrade

Consider these pointers before you upgrade the Hosted Collaboration Media Fulfillment to the latest version:

- Ensure that you have a valid DRF backup of your HCM-F Cluster.

  Note Cisco does not support and cannot guarantee that a VMware snapshot can be used to successfully restore Cisco Hosted Collaboration Media Fulfillment application. If you cannot restore the application from a snapshot, your only recourse is to reinstall older version of the Hosted Collaboration Media Fulfillment application and restore using the DRF backup.

- Check the network connectivity.
- Ensure to stop all the sync services.
- Ensure that there are no expired certificates including the trust certificates for the services.

  To list all certificates, run the **show cert list own** and run the **show cert list trust** commands.

  To verify if the own certificates are valid, run the **show cert own <cert name>** command through the CLI on the Cisco HCM-F platform. Check the validity field for the certificate validity information. For example: **show cert own tomcat/tomcat.pem**.

  To check if the trust certificates are valid, run the **show cert trust <filename>** command.

  Based on the certificate issuer, you can regenerate the certificates. To regenerate the self-signed certificate, use the **set cert regen <name>** command. For CA signed certificate, generate CSR using the **set csr gen**

<name> command, get it signed by a CA and upload the certificates using the **set cert import <name>** command.

The following are examples of the system security certificates that you can regenerate.

Own Certificates

- tomcat
- ipsec
- tomcat-ECDSA
- ITLRecovery
- authz

Upgrade Overview

The following Cisco HCM-F upgrade paths are supported:

- 11.5(x) to 12.5(1) and later Service Update releases
- 10.6(x) to 12.5(1) and later Service Update releases

Note After you upgrade to 12.5 release, you can revert to an older software version using the switch version option. However, you cannot upgrade to any pre-12.5 release. Use PCD migration or cluster rebuild, if it is necessary to upgrade to any pre-12.5 version.

Upgrade the Cisco HCM-F Application Node before upgrading any Cisco HCM-F Web Services Nodes.

Before you begin the upgrade process, obtain the appropriate upgrade file using one of the following methods:

- Use the Product Upgrade Tool (PUT). To use the PUT, navigate to https://tools.cisco.com/gct/Upgrade/jsp/index.jsp. Enter your Cisco contract number (Smartnet, SASU or ESW) and request the DVD set.
- Purchase the upgrade from Cisco Sales if you don't have a contract for Cisco HCS.

In general, perform the following tasks to upgrade Cisco HCM-F:

- Upgrade Cisco HCM-F
- Validate the Cisco HCM-F Upgrade
- Update the HCM-F Version in Cisco Unified CDM
- Update the Guest operating System

Upgrade Cisco HCM-F

Before upgrading an HCM-F cluster containing an Application Node and Web Services (WS) Nodes, perform the following tasks:

1. Ensure that you have a valid DRF backup of your HCM-F Cluster.
2. On the Application Node CLI, run **show hcs cluster nodes**. Verify that the versions of the Application Node and WS Nodes are correct.
3. On the Application Node CLI, run **show hcs cluster verify detailed**. Verify that all WS Nodes in the cluster are reachable and show `Configurations VERIFIED`.
4. If you use Prime Collaboration Assurance, review and perform the task (Enabling HCM-F and Prime Collaboration Assurance to Communicate) in the *Cisco Hosted Collaboration Solution Install Guide* if necessary. The *Cisco Hosted Collaboration Solution Install Guide* is available at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html.

Note

- If Cisco HCM-F 10.6(3) SU1 was previously installed, skip to Upgrade a Multinode Environment.

Note

- Upgrade the Application Node and let the upgrade complete before upgrading any WS Nodes attached to it. If you do not switch versions during the upgrade, run the **utils system switch-version** command on the Application Node before running it on the WS Nodes.
- If you are running RTMT and monitoring performance counters during a Cisco HCM-F upgrade, the performance counters are not updated during and after the upgrade. To continue accurate monitoring of performance counters after the upgrade is finished, either reload the RTMT configuration profile or restart RTMT.

Use this procedure to upgrade a Cisco HCM-F Application Node or a Cisco HCM-F Web Services Node.

Procedure

Step 1 Obtain the upgrade media to upgrade the Cisco HCM-F platform.

If you downloaded the software executable from Cisco.com, do one of the following:

- Prepare to upgrade from a local folder:
  a. Copy the Cisco HCM-F upgrade file to a temporary folder on your local hard drive.
  b. Open an SFTP client and connect to the Cisco HCM-F server using the adminsftp user ID and password that you set up during installation.
  c. Navigate to the upgrade folder by entering **cd upgrade**.
  d. Type **put** <*upgrade filename*> to transfer the file.

- Prepare to load an ISO file:
  a. Copy the Cisco HCM-F upgrade ISO to a data store accessible by the virtual machine.
  b. Attach the ISO image to the virtual machine's DVD drive.
- Put the upgrade file on an FTP or SFTP server that the server that you are upgrading can access. Copy the contents of the upgrade disk or downloaded upgrade files to the remote server. Make sure that the Cisco HCM-F upgrade file filename begins with HCS.

Step 2 On the virtual machine that you are upgrading, log in to the Cisco HCM-F CLI and enter **utils system upgrade initiate**.

Step 3 Choose the source from which you want to upgrade:

- 1—Remote Filesystem using SFTP
- 2—Remote Filesystem using FTP
- 3—Local DVD
- 4—Local Upload Directory

Step 4 Follow the system prompts for the upgrade option that you chose.

Step 5 The system prompts you when the upgrade process is complete. If you did not choose to automatically switch versions, enter **utils system switch-version**. Then enter **`yes`** to confirm that you want to reboot the server and switch to the new software version.

Step 6 After the upgrade completes, log in to the Cisco HCM-F CLI.

- Enter **show version active** to verify that the current version is the upgraded version.
- Post HCM-F upgrade, change the users password for the GUI access.

Step 7 Perform this step if you used the **utils system switch-version** command in Step 5, on page 4. After the Application node and all WS Nodes have switched versions, log in to the Application Node CLI and run the **set hcs cluster config** command.

Step 8 From the HCM-F CLI, run the **utils service list** command to view the services. Run the **utils service start** *service_name* command to restart any services that were stopped before the upgrade.

Validate the Cisco HCM-F Upgrade

Procedure

Step 1 Verify that no error logs were created during or after the upgrade.

Step 2 Verify that the active version shows the correct upgraded version by running the **show version active** CLI command.

Step 3 Verify that all services are running as they were before the upgrade by running the **utils service list** CLI command.

Step 4 Verify that the administration GUI is accessible and displays the correct upgraded version by clicking the **About** link after logging in.

Step 5 Verify that all the syncs (for example, Service Provider, Data Center, vCenter, Customer, UCS Manager) were successful.

Step 6 Verify that Hosted License Manager does not contain any post-upgrade errors and that licenses are assigned to the proper customer.

Step 7 Verify that Platform Manager or Prime Collaboration Deployment is running (whichever you used for the upgrade).

Step 8 Verify that Cisco HCS North Bound Interface Web Service is running.

Step 9 Verify that Service Inventory is running.

Step 10 After upgrading the Application and Web Services nodes, log in to the CLI on the Application node. Verify that the Application and Web Services nodes are at the correct version. Run the following command: **show hcs cluster nodes**.

You can troubleshoot a situation in which a node upgrade appears to have completed successfully at the console, but the output of **show hcs cluster nodes** does not indicate the upgrade version. For more information, see Cluster Node Version Mismatch .

Update the HCM-F Version in Cisco Unified CDM

After you upgrade Cisco HCM-F, update the version of HCM-F in Cisco Unified Communications Domain Manager (Unified CDM). Updating the version involves the Unified CDM user interface and the Unified CDM command-line interface.

Note Cisco HCM-F will deprecate the support of Cisco Unified Communications Domain Manager in the upcoming releases with limited support for existing integration, Cisco HCS partners and customers are advised to take necessary steps to align their requirements.

1. Take the following steps in the Unified CDM interface.
   a. Log in to Unified CDM as hcsadmin.
   b. Navigate to **Device Management** > **HCM-F**.
   c. Select the HCM-F device.
   d. In the **HCM-F Version** field, select the release version.
   e. Click **Save**.
2. In the Unified CDM command-line interface, run the following command: **app start voss-deviceapi**.

Important The command enables the **Server Type** field on the Base tab. The field is required when you add a UC application, such as Cisco Unified Communications Manager, or when you upgrade a UC application. The command also displays the **Version** field on the Publisher tab. If you do not run the command after you upgrade HCM-F, you cannot then add or update UC applications.

Update the Guest Operating System

After completing the upgrade and verifying that the cluster has upgraded, update the Guest Operating System on the VMs. Perform the following procedure for each node in the cluster.

Procedure

Step 1 From the CLI, run the **utils system shutdown** command.

Step 2 Access the vSphere client and verify that the VM is powered off.

Step 3 Select the VM and click **Edit virtual machine settings**.

Step 4 In the Virtual Machine Properties window, click the **Options** tab.

Step 5 For Guest Operating System Version, select **Red Hat Enterprise Linux 6 (64-bit)**.

Step 6 Click **OK**.

Step 7 Power on the VM.

Migrating from Cisco Unified Operations Manager to Cisco Prime Collaboration Assurance

You can migrate the monitoring application from Cisco Unified Operations Manager to Cisco Prime Collaboration Assurance. Use the Migration Utility Tool from the CLI, or use the Infrastructure Manager user interface within Cisco HCM-F.

Migrate Using the Migration Utility Tool

Use this procedure to migrate one instance of Cisco Unified Operations Manager to one instance of Cisco Prime Collaboration Assurance.

Procedure

Step 1 Enable the Cisco HCS DMA-SA Service. From the CLI, run the **utils service activate Cisco HCS DMA-SA Service** command.

Step 2 Define the Cisco Prime Collaboration Assurance application in Cisco HCM-F.

a) From the Infrastructure Manager interface, select **Application Management** > **Management Application**.
b) Click **Add New**.
c) In the Application Type field, select **Prime Collaboration**.
d) Enter a name in the Name field.
e) (Optional). Provide a description and select the virtual machine.
f) Click **Save**.
g) Open **Credentials** and click **Add New**. Specify credentials for **ADMIN** and **SFTP** Credential Types.

h) Open **Network Addresses** and click **Add New**. Select **Service Provider Space** as the Network Space and specify the IP address, hostname, and domain of the HCM-F server.
i) Click **Save**.

Step 3 From the CLI, run the **utils migrate cuom_to_primecollab** command.

Step 4 Provide the names of the Cisco Unified Operations Manager and Cisco Prime Collaboration Assurance when prompted.

Migrate Using the Infrastructure Manager User Interface

Use the Infrastructure Manager user interface to change the monitoring application from Cisco Unified Operations Manager to Cisco Prime Collaboration Assurance.

Note The Cisco Prime Collaboration Assurance specified for a Customer monitors the Customer's clusters and equipment, unless overridden by a different Cisco Prime Collaboration Assurance specified at the cluster or equipment level. Cisco recommends that you have one instance of Cisco Prime Collaboration Assurance manage all devices and clusters belonging to a Customer. Therefore, steps 3 and 4 of the following procedure are not typically required.

Procedure

Step 1 Enable the Cisco HCS DMA-SA Service. From the CLI, run the **utils service activate Cisco HCS DMA-SA Service** command.

Step 2 Define the Cisco Prime Collaboration Assurance application in Cisco HCM-F.

a) From the Infrastructure Manager interface, select **Application Management** > **Management Application**.
b) Click **Add New**.
c) In the Application Type field, select **Prime Collaboration**.
d) Enter a name in the Name field.
e) Optionally provide a description and select the virtual machine.
f) Click **Save**.
g) Open **Credentials** and click **Add New**. Specify credentials for ADMIN and SFTP credential types.
h) Open **Network Addresses** and click **Add New**. Select **Service Provider Space** as the Network Space and specify the IP address, hostname, and domain of the HCM-F server.
i) Click **Save**.

Step 3 To update the Monitoring Application for a Customer:

Note To migrate all customers automatically, run the **set hcs link auto-primecollab-linkage enable** command from the CLI before performing steps a through e.

a) From the Infrastructure Manager interface, select **Customer Management** > **Customer**.
b) Click the customer you want to update.
c) In the Application Monitoring this Customer field, select your Cisco Prime Collaboration Assurance application.
d) Click **Save**.

e) To monitor data migration job status, select **Administration** > **Jobs**.

Step 4 To update the Monitoring Application for Customer Equipment:

a) From the Infrastructure Manager interface, select **Customer Management** > **Customer** > **Customer Location** > **Customer Equipment**.
b) Click the customer equipment you want to update.
c) In the Application Monitoring this Customer Equipment field, select your Cisco Prime Collaboration Assurance application.
d) Click **Save**.

Step 5 To update the Monitoring Application for a Cluster:

a) From the Infrastructure Manager interface, select **Cluster Management** > **Cluster**.
b) Click the cluster you want to update.
c) In the Application Monitoring this Cluster field, select your Cisco Prime Collaboration Assurance application.
d) Click **Save**.