Install HCM-F

Installation Overview for Cisco HCM-F

This section covers the installation of an HCM-F Application Node and one or more HCM-F Web Services Nodes.

Before you proceed with the installation, consider the following requirements and recommendations:

- Cisco HCM-F 11.5(2) and later provides an enhanced autovacuum functionality. The autovacuum frequently runs in background and cleans up the old deleted rows (dead tuples) from the database tables.
- Ensure that you enable Network Time Protocol (NTP) on the Cisco HCM-F server. To verify the NTP status, log in to the Cisco HCM-F command line interface, and enter **utils ntp status**.
- If you are installing multiple HCM-F nodes:
  - Ensurethat all nodes point to the same NTP server.
  - Ensure you are consistent with using either Domain Network Server (DNS) or non-DNS across all nodes.
- Be aware that when you install on an existing server, the hard drive gets formatted and all existing data on the drive gets overwritten.
- Install Cisco HCM-F using static IP addressing to ensure that the Cisco HCM-F obtains a fixed IP address.
- Don't attempt to perform any configuration tasks during the installation.
- Don't install any Cisco-verified applications until you complete the installation.

Navigating the Installation Wizard

Table 1: Installation Wizard Navigation

To Do This	Press This
Move to the next field	**Tab**
Move to the previous field	**Alt-Tab**
Choose an option	Space bar or **Enter**
Scroll up or down in a list	**Up Arrow** or **Down Arrow** key
Go to the previous window	Space bar or **Enter** to choose **Back** (when available)
Get help information for a window	Space bar or **Enter** to choose **Help** (when available)

Install the HCM-F Application Node

Procedure

Step 1 Insert the Cisco HCM-F ISO disk into the DVD drive of the virtual machine.

Step 2 Reboot and start the virtual machine.
The HCM-F installation wizard opens.

Step 3 On the **Media Check** screen, select **OK** to perform a check of the media, or select **Skip** to proceed to the installation.

Step 4 On the **Product Deployment Selection** screen, select **HCS Application Suite** and then select **OK**.

Step 5 On the **Proceed with Install** screen, verify that you are installing the version you want, and select **Yes** to overwrite the hard drive.

Step 6 On the **Platform Installation Wizard** screen, select **Proceed**.

Step 7 On the **Basic Install** screen, select **Continue**.

Step 8 On the **Timezone Configuration** screen, select your time zone from the menu, and then select **OK**.

Step 9 On the **Auto Negotiation Configuration** screen, select **Continue**.

Step 10 On the **MTU Configuration** screen, select **No** to leave the MTU size at the OS default, or select **Yes** and enter new values.

Step 11 On the **DHCP Configuration** screen, select **No** to use a static IP address.

Step 12 On the **Static Network Configuration** screen, specify the **Hostname**, **IP Address**, **IP Mask**, and **GW Address** for the App Node, and select **OK**.

The virtual machine must be able to reach the gateway that is entered for the static configuration, or else the installation will give an error and not proceed.

Step 13 On the **DNS Client Configuration** screen:

- Select **Yes** to use DNS. Enter values for the **Primary DNS**, **Secondary DNS (optional)**, and **Domain**.
- Select **No** to not use DNS.

If the virtual machine cannot reach the DNS server, then the installation gives an error and does not proceed.

Step 14 On the **Administrator Login Configuration** screen, set up the **Administrator ID** and **Password** for the App Node. Then select **OK**.

Step 15 On the **Certificate Information** screen, enter values for **Organization**, **Unit**, **Location**, and **State.** Select **Country** from the menu. Then select **OK**.

Step 16 On the **Network Time Protocol Client Configuration** screen, enter the hostname or IP address for one to five NTP Servers. Then select **OK**.

Step 17 On the **Security Configuration** screen set the system security password for the App Node. Then select **OK**.

Step 18 On the **Platform Configuration Confirmation** screen, select **OK**.

After the application node is installed, the virtual machine is rebooted. The following message appears, and you are prompted to log in to the Application Node: `The installation of HCS Application Suite has completed successfully`.

What to do next

Set the minimum version of the Transport Layer Security (TLS) protocol for the application node from the command line with **set tls min-version <version>**. This command disables all the lower version of TLS than the set version. For example, if you set the minimum version as TLSv1.2, then the TLSv1.1 and the below version is disabled.

Note

- Ensure that your web browser supports the TLS version you have set.
- Ensure that any client application using HCMF NBI APIs also support the minimum TLS version you have set.

Install the Remote Access Portal Node

Procedure

Step 1 Insert the Cisco HCM-F ISO disk into the DVD drive of the virtual machine.

Step 2 Reboot and start the virtual machine.
The HCM-F installation wizard opens.

Step 3 On the **Media Check** screen, select **OK** to perform a check of the media, or select **Skip** to proceed to the installation.

Step 4 On the **Product Deployment Selection** screen, select **HCS Remote Access Portal** and then select **OK**.

Step 5 On the **Proceed with Install** screen, verify that you are installing the version you want, and select **Yes** to overwrite the hard drive.

Step 6 On the **Platform Installation Wizard** screen, select **Proceed**.

Step 7 On the **Basic Install** screen, select **Continue**.

Step 8 On the **Timezone Configuration** screen, select your time zone from the menu, and then select **OK**.

Step 9 On the **Auto Negotiation Configuration** screen, select **Continue**.

Step 10 On the **MTU Configuration** screen, select **No** to leave the MTU size at the OS default, or select **Yes** and enter new values.

Step 11 On the **DHCP Configuration** screen, select **No** to use a static IP address. Select **Yes** to use DHCP to obtain an IP address.

Step 12 On the **Static Network Configuration** screen, specify the **Hostname**, **IP Address**, **IP Mask**, and **GW Address** for the Remote Access Portal Node and select **OK**.

The virtual machine must be able to reach the gateway that is entered for the static configuration, or else the installation will give an error and not proceed.

Step 13 On the **DNS Client Configuration** screen:

- Select **Yes** to use DNS. Enter values for the **Primary DNS**, **Secondary DNS (optional)**, and **Domain**.
- Select **No** to not use DNS.

If the virtual machine cannot reach the DNS server, then the installation gives an error and does not proceed.

Step 14 On the **Administrator Login Configuration** screen, set up the **Administrator ID** and **Password** for the Remote Access Portal Node. Then select **OK**.

Step 15 On the **Certificate Information** screen, enter values for **Organization**, **Unit**, **Location**, and **State.** Select **Country** from the menu. Then select **OK**.

Step 16 On the **Network Time Protocol Client Configuration** screen, enter the hostname or IP address for one to five NTP Servers. Then select **OK**.

Step 17 On the **Security Configuration** screen set the system security password for the Remote Access Portal Node. Then select **OK**.

Step 18 On the **Platform Configuration Confirmation** screen, select **OK**.
After the Remote Access Portal Node is installed, the virtual machine is rebooted. The following message appears and you are prompted to log in to the Remove Access Portal Node: `The installation of HCS Remote Access Portal has completed successfully`.

Step 19 Log in to the CLI and run the **utils service activate** <*service_name*> command to activate the following services required by the RAP node:

- Cisco HCS RAP API Service
- Cisco HCS RAP SSO Service
- Cisco HCS RAP WWW Service
- Cisco HCS RAP Help Service

Install HCM-F Real Time Monitoring Tool

This section describes about the HCM-F Real Time Monitoring Tool (RTMT), uninstalling RTMT from Windows, and uninstalling RTMT from Red Hat Linux.

Install HCM-F Real Time Monitoring Tool

The Cisco HCM-F installation consists of one HCM-F application server. One copy of RTMT installed on your computer lets you monitor one HCM-F server at a time. To monitor HCM-F on a different server, you must log out of the RTMT session on the first server before you can log in to the other HCM-F server.

Before you install RTMT, consider the basics on HCM-F RTMT.

- HCM-F RTMT monitors only HCM-F Servers.
- HCM-F RTMT can be the only version of RTMT run on a client computer.

Procedure

Step 1 From the command line, run the **utils service list** command to verify that the Cisco AMC Service is running.

The Cisco AMC Service allows RTMT to retrieve real-time information from the HCM-F server.

Step 2 Log in to HCM-F on the application server.

Step 3 In HCM-F, click the **Infrastructure Manager** tab.

Step 4 Navigate to **Administration** > **HCM-F RTMT Installers**.

The HCM-F RTMT Installers page opens.

Step 5 Perform one of the following steps:

- To download RTMT for a client computer that is running the Microsoft Windows operating system, click **HCM-F RTMT Windows Installer**.
- To download RTMT for a client computer that is running the Linux operating system, click **HCM-F RTMT Linux Installer**.

Step 6 Save the executable in the preferred location on your computer.

Step 7 Perform one of the following steps to install RTMT:

- To install the Windows version, double-click the RTMT icon that appears on the desktop or locate the directory to which you downloaded the file and run the RTMT installation file. The extraction process begins, and then the RTMT Introduction window appears.

  Note If you are installing RTMT on a Windows Vista computer, the following User Account Control popup message appears: "An unidentified program wants to access your computer." To continue, click **Allow**.

- To install the Linux version, ensure that the file has execute privileges. For example, enter the following command, which is case sensitive: **chmod +x CcmServRtmtPlugin.bin**. The RTMT Introduction window opens.

Step 8 Click **Next**.

Step 9 To accept the license agreement, click **I accept the terms of the License Agreement** and then click **Next**.

Step 10 Perform one of the following steps:

- Click **Next** to accept the default folder.

  The default installation paths are:

- Windows: `C:/Program Files/Cisco/HCS/JRtmt`
- Windows 7 32 bit: `C:/Program Files/Cisco/HCS/JRtmt`
- Windows 7 64 bit: `C:/Program Files (x86)/Cisco/HCS/JRtmt`
- Linux: `/opt/Cisco/HCS/JRtmt`

- If you do not want to use the default folder, click **Choose** and navigate to a different folder. Then click **Next**.

The selected folder must be empty. If the selected folder is not empty, a warning dialog appears and you cannot proceed unless you select or create an empty folder.

If the installer detects that RTMT is already installed on the computer, a warning dialog appears. You cannot have more than one copy of RTMT installed on the same computer. Click **Continue**. The uninstaller starts and the Uninstall Real-Time Monitoring Tool window appears. Click **Uninstall**, allow the uninstallation to finish, and then click **Done**. You may be prompted to restart the computer.

Step 11 On the Pre-Installation Summary page, review the information, and then click **Install**.

The installation begins. Do not click **Cancel**.

Step 12 To close the installer, click **Done**.

Uninstall RTMT for Windows

User preferences and the module jar files for RTMT (the cache) are saved locally on the client computer. When you uninstall RTMT, you can delete or save the cache.

Procedure

Select **Start** > **Settings** > **Control Panel** > **Add/Remove Program** and follow the instructions.

Note If you are uninstalling RTMT in Windows Vista, the following User Account Control message appears: `An unidentified program wants to access your computer`. To continue, click **Allow**.

Uninstall RTMT for Red Hat Linux

You can uninstall RTMT on Red Hat Linux with KDE or a Gnome client.

Procedure

Select **Start** > **Accessories** > **Uninstall Real-Time Monitoring Tool** from the task bar and follow the instructions.

Note Alternatively, you can run `/opt/Cisco/HCS/JRtmt/Uninstall_Real-Time Monitoring Tool X.X/Uninstall Real-Time Monitoring Tool X.X`.

Install Security Certificates

This section enables you to install RSA and ECDSA certificates.

Install RSA Certificates

Before you begin

- Use Certificate Authority (CA) signed certificates
- Use CA that supports RSA algorithm
- Follow these recommendation when you obtain a HCMF server certificate from a Certificate Authority (CA). Refer to the table for detailed information on the normative references.

1. Restrict X.509 certificate validity period.
2. Use certificates from qualified CA.
3. Support OCSP revocation and OCSP stapling.
4. Generate and present X.509 certificates properly.

Requirement	Normative References
Restrict X.509 certificate validity periods	Do not request or generate certificates with excessively long lifetimes. Normative references RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
Use certificates from qualified CA	Cisco Cryptographic Controls Policy.

Requirement	Normative References
Support OCSP revocation and OCSP stapling	Support OCSP for X.509 certificate revocation. Support OCSP stapling in TLS. Apply reasonable caching and validation policies. Control keys can be used to sign OCSP responses. Normative references RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP". RFC 6066: "TLS Extension Definitions" (Section 8: Certificate Status Request). RFC 6961: "Multiple Certificate Status Request Extension". RFC 6818: "Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". RFC 6125: "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)". RFC 6698: "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA".
Generate and present X.509 certificates	When requesting X.509 certificates from CAs or presenting them to relying parties, follow the standard practices, as well as miscellaneous practices not covered in other requirements. This applies to TLS and any other place where X.509 is used. Normative references RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" (aka PKIX). RFC 6818: "Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". RFC 6125: "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)".

Procedure

Step 1 Log in to the Cisco HCM-F CLI as an administrator.

Step 2 Generate the Certificate Signing Request (CSR).

```
admin:set csr gen tomcat-RSA
```

Step 3 Ensure that the CSR is generated successfully.

```
admin:show csr list tomcat-RSA
```

Step 4 Send the CSR to CA.

```
admin:show csr own tomcat-RSA
```

Step 5 Import the new certificate:

a) Import the Root Certificate to the trust store:

```
set cert import trust tomcat-RSA
```

b) Import the Server Certificate to the own store:

```
set cert import own tomcat-RSA
```

Step 6 Enter the certificate when the CLI prompts.

Step 7 Restart tomcat.

```
utils service restart Cisco Tomcat
```

Install ECDSA Certificates

HCM-F 11.5(1) and above supports ECDSA certificates. Modern browsers prefer newer ECDSA algorithm certificates rather than RSA when negotiating a secure connection to the web interface of HCM-F. If you only upload an RSA certificate, when ECDSA is negotiated, a certificate warning appears because the self signed certificate is still being used. Server presents self-signed ECDSA certificate even though you uploaded the RSA CA trusted certificate.

Before you begin

- Use Certificate Authority (CA) signed certificates
- Use CA that supports EC algorithm, and Subject Alternative Name (SAN)
- Use a browser that requests EC certificates

Note

- Google Chrome and Mozilla firefox prefers ECDSA ciphers over RSA ciphers.
- Internet Explorer, version 11 prefers RSA ciphers over ECDSA ciphers.

Note HCM-F doesn't support enabling/disabling EDCSA certificate. If you can't or doesn't want to generate ECDSA certificates, contact Cisco Technical Assistance Center (TAC) for assistance.

Procedure

Step 1 Log in to the Cisco HCM-F CLI as an administrator.

Step 2 Generate the Certificate Signing Request (CSR).

```
admin:set csr gen tomcat-ECDSA
```

Step 3 Ensure that the CSR is generated successfully.

```
admin:show csr list tomcat-ECDSA
```

The CLI displays the CSR.

Step 4 Send the CSR to CA.

```
admin:show csr own tomcat-ECDSA
```

Note Update CA with server hostnames that must be added to SAN.

Step 5 Import the new certificates:

a) Import the Root Certificate to the trust store:

```
set cert import trust tomcat-ECDSA
```

b) Import the Server Certificate to the own store:

```
set cert import own tomcat-ECDSA
```

Step 6 Enter the new certificate when the CLI prompts.

Step 7 Restart tomcat.

```
utils service restart Cisco Tomcat
```

What to do next

To verify the successful installation of ECDSA, ensure that the common name of certificate is updated as *Hostname*-EC-*Domain_Name*.