Troubleshooting and Monitoring

This chapter contains information on the following topics:

Troubleshooting Installation

Use the following sections to troubleshoot problems that occur during installation of the Cisco HCM-F:

Handling Network Errors During Installation

During the installation process, the installation program verifies that the server can successfully connect to the network by using the network configuration that you enter. If the server cannot connect, a message appears; you get prompted to select one of the following options:

- **RETRY**—The installation program tries to validate networking again. If validation fails again, the error dialog box appears again.

- **REVIEW (Check Install)**—This option allows you to review and modify the networking configuration. When this option is detected, the installation program returns to the network configuration windows.

  Networking gets validated after you complete each networking window, so the message may appear multiple times.

- **HALT**—The installation stops. You can copy the installation log files to a USB disk to aid troubleshooting of your network configuration.

- **IGNORE**—The installation continues. The networking error gets logged. In some cases, the installation program validates networking multiple times, so this error dialog box may appear multiple times. If you choose to ignore network errors, the installation may fail.

Examining Log Files

If you encounter problems with the installation, you may be able to examine the installation log files by entering the following commands in command line interface.

To obtain a list of install log files from the command line, enter

CLI> **file list install ***

To view the log file from the command line, enter

CLI> **file view install** *log_file*

where:

log_file specifies a log file name having the format: install_log_YYYY-MM-DD.HH.MM.SS.log in which the date and time of the log file is the time at which the install or the upgrade was initiated on the system.

You can get more information about installation events by viewing or downloading the System History log. See the following for more information:

System History Log, page 10-1

Troubleshooting HCM-F Components

Use the following sections to troubleshoot problems with Cisco HCM-F components:

- Troubleshooting for Cisco HCS Shared Data Repository, page 12-2
- Troubleshooting Cisco HCS CUCDMSync Service, page 12-3
- Common CUCDMSynch Issues, page 12-4
- Troubleshooting Cisco HCS Fulfillment Service, page 12-5
- Troubleshooting Cisco Domain Manager Adapter for the Cisco Unified Operations Manager (CUOM), page 12-6
- Troubleshooting Service Inventory, page 12-8
- Troubleshooting Cisco HCS Platform Manager Service, page 12-11
- Troubleshooting Cisco HCM-F Administrative Interface, page 12-12
- Troubleshooting Cisco HCS North Bound Interface Web Service API, page 12-13

Troubleshooting for Cisco HCS Shared Data Repository

Table 12-1 on page 12-3 lists the troubleshooting steps to perform for Shared Data Repository.

Table 12-1   Troubleshooting Checklist for Shared Data Repository

	Task	For More Information
Step 1	Check to see that the **Cisco CDM Database** Service is still running.	Services on the Cisco HCM-F Platform, page 3-1
Step 2	Check the log files. • The **activelog cdm/api** logs contain only POJO API logs. Each service has its own log file. Cisco recommends to use these log files to investigate only issues that are not service-specific. • The **activelog cdm/database** logs contain database transaction logs	Managing Traces on the Cisco HCM-F Platform, page 12-15 Table 12-11 on page 12-16

Troubleshooting Cisco HCS CUCDMSync Service

Table 12-2 on page 12-3 lists the troubleshooting steps to perform for CUCDMSync Service.

Table 12-2   Troubleshooting Checklist for CUCDMSync Service

	Task	For More Information
Step 1	Check to see that the following services are running: • Cisco CDM Database • Cisco JMS Broker • Cisco Tomcat • Cisco HCS Admin UI • Cisco HCS CDM UI • Cisco HCS Fulfillment Service • Cisco HCS CUCDMSync Service	Services on the Cisco HCM-F Platform, page 3-1
Step 2	Check that the configuration in Infrastructure Manager is correct.	Configuration Checklist for CUCDM Sync Services, page 7-6
Step 3	Check the diagnostics information for the CUCDMSync Service.	utils diagnose hcs, page 10-93
Step 4	Run a manual CUCDMSync and check the job results.	Performing a Manual Sync, page 7-14 Viewing Jobs, page 7-15

Table 12-2   *Troubleshooting Checklist for CUCDMSync Service*

	Task	For More Information
Step 5	Check the CUCDMSync alarms that are located in **activelog syslog/CiscoSyslog**.	Managing Alarms on the Cisco HCM-F Platform, page 12-14 Table 12-10Alarm CLI Commands, page 12-14 For information on individual alarms, see the *Alarm Catalogs for Cisco Hosted Collaboration Mediation Fulfillment.*
Step 6	Check the CUCDMSync log files that are located in **activelog hcs/cucdmsync**.	Managing Traces on the Cisco HCM-F Platform, page 12-15 Table 12-11Trace CLI Commands, page 12-16

Common CUCDMSynch Issues

The following sections details common CUCDMSync errors.

Issue: Sync Request has a Job Status of Fail

Symptom: Unable to perform manual or automatic sync request.

Resolution: Check that CUCDMSync is configured correctly; see the "Configuration Checklist for CUCDM Sync Services" section on page 7-6.

Troubleshooting Cisco HCS VCenterSync Service

Table 12-3 on page 12-4 lists the troubleshooting steps to perform for VCenterSync Service.

Table 12-3   *Troubleshooting Checklist for VCenterSync Service*

	Task	For More Information
Step 1	Check to see that the following services are running: • Cisco CDM Database • Cisco JMS Broker • Cisco Tomcat • Cisco HCS Admin UI • Cisco HCS CDM UI • Cisco HCS Fulfillment Service • Cisco HCS VCenterSync Service	Services on the Cisco HCM-F Platform, page 3-1
Step 2	Check that VCenterSync configuration is correct.	Configuration Checklist for vCenter Sync Services, page 7-6

Table 12-3   *Troubleshooting Checklist for VCenterSync Service*

	Task	For More Information
Step 3	Check the diagnostics information for the VCenterSync Service.	utils diagnose hcs, page 10-93
Step 4	Run a manual VCenterSync and check the job results.	Performing a Manual Sync, page 7-14 Viewing Jobs, page 7-15
Step 5	Check the VCenterSync alarms located in **activelog syslog/CiscoSyslog**.	Managing Alarms on the Cisco HCM-F Platform, page 12-14 Table 12-10Alarm CLI Commands, page 12-14 For information on individual alarms, see the *Alarm Catalogs for Cisco Hosted Collaboration Mediation Fulfillment.*
Step 6	Check the VCenterSync log files located in **activelog hcs/vcentersync**.	Managing Traces on the Cisco HCM-F Platform, page 12-15 Table 12-11Trace CLI Commands, page 12-16

Troubleshooting Cisco HCS Fulfillment Service

Table 12-5 on page 12-6 lists the troubleshooting steps to perform for the Fulfillment Service.

Table 12-4   *Troubleshooting Checklist for Fulfillment Service*

	Task	For More Information
Step 1	Check to see that the following services are running: • Cisco CDM Database • Cisco JMS Broker • Cisco HCS Fulfillment Service	Services on the Cisco HCM-F Platform, page 3-1
Step 2	Check the HCS Fulfillment Auto-VM-Linkage parameter.	show hcs fulfillment auto-vm-linkage, page 10-60
Step 3	Check the diagnostics information for the Fulfillment Service.	utils diagnose hcs, page 10-93

Table 12-4   Troubleshooting Checklist for Fulfillment Service

	Task	For More Information
Step 5	Check the Fulfillment alarms located in **activelog syslog/CiscoSyslog**.	Managing Alarms on the Cisco HCM-F Platform, page 12-14 Table 12-10Alarm CLI Commands, page 12-14 For information on individual alarms, see the *Alarm Catalogs for Cisco Hosted Collaboration Mediation Fulfillment.*
Step 6	Check the Fulfillment log files located in **activelog hcs/fulfillment**.	Managing Traces on the Cisco HCM-F Platform, page 12-15 Table 12-11Trace CLI Commands, page 12-16

Troubleshooting Cisco Domain Manager Adapter for the Cisco Unified Operations Manager (CUOM)

Table 12-5 on page 12-6 lists the troubleshooting steps to perform for DMA-CUOM Service.

Table 12-5   Troubleshooting Checklist for DMA-CUOM

	Task	For More Information
Step 1	Check to see that the following services are running: • Cisco CDM Database • Cisco JMS Broker • Cisco Tomcat • Cisco HCS Fulfillment Service • Cisco HCS DMA-CUOM Service	Services on the Cisco HCM-F Platform, page 3-1
Step 2	Check the diagnostics information for the DMA-CUOM Service.	utils diagnose hcs, page 10-93

Table 12-5   Troubleshooting Checklist for DMA-CUOM

	Task	For More Information
Step 3	Check the DMA-CUOM alarms located in **activelog syslog/CiscoSyslog**.	Managing Alarms on the Cisco HCM-F Platform, page 12-14 Table 12-10Alarm CLI Commands, page 12-14 For information on individual alarms, see the *Alarm Catalogs for Cisco Hosted Collaboration Mediation Fulfillment.*
Step 4	Check the DMA-CUOM log files located in: • **activelog tomcat/logs/dmacuom/log4j** which includes communication with fulfillment and CUOM logs. • **activelog tomcat/logs/dmacuom/catalina.out** which contains DMA-CUOM exceptions.	Managing Traces on the Cisco HCM-F Platform, page 12-15 Table 12-11Trace CLI Commands, page 12-16

Common DMA-CUOM Issues

The following sections details common DMA-CUOM errors.

Issue: Missing Required Data

Symptom: New device or device change not propagated to CUOM.

Resolution: Ensure that all required data in the following list is configured for the device:

- Assigned CUOM
- Assigned using HCS GUI (or HCS NBI or cdmcli)
- Assigned the default CUOM at Customer level
- Overrode the default for applications at Cluster level
- Overrode the default for CPE on individual customer equipment devices
- Assigned CUOM must have: SP_SPACE network address
- Provided CredentialType=ADMIN credential (defined in default credentials or for the specific device)
- Assigned Network Addresses (automatically synced for applications and CPE)
- Assigned SP_SPACE: IP & hostname sent to CUOM as system IP & hostname
- Assigned APPLICATION_SPACE: IP & hostname are sent to CUOM as private IP & hostname
- Provided Credentials Selection rules (READ-ONLY is required, READ-WRITE is optional). Note: Multiple credentials for same device can be included.

Issue: CUOM NBI Down

Symptom: DMA-CUOM unable to add devices to CUOM.

Resolution: Start the Northbound Interface process (OrionNBI) by doing the following:

Step 1   Open cmd window on CUOM server.

Step 2   Enter the following commands:

> *net stop OMHealthMonitor*
>
> *cd C:\Program Files\CSCOpx\bin\footprint*
>
> *perl EnableNBI.pl "C:\Program Files\CSCOpx"*
>
> *net stop CRMDMgt*
>
> *dnet start CRMDMgtd*
>
> *net start OMHealthMonitor*

Issue: CUOM Restarted

Symptom: DMA-CUOM unable to add devices to CUOM.

Background: CUOM cannot process service requests for 20-30 minutes after a restart.

Resolution: This issue should resolve itself after 20-30 minutes.

Issue: IPV6

CUOM is not supported on an IPv6 host.

Symptom: Random behavior, such as some devices are not added or periods during which CUOM does not accept requests.

Resolution: Perform the following:

Step 1   Check whether IPv6 is enabled: At cmd prompt enter: **ipconfig | find "IPv6"**

Step 2   Disable IPv6 on all network interfaces: **Start > Control Panel > Network and Sharing Center**.

Step 3   Click **Manage Network Interfaces**.

Step 4   Right-click a **Network Interface**, select **Properties**.

Step 5   Click the **Networking** tab.

Step 6   Uncheck **Internet Protocol Version 6 (TCP/IPv6)**.

Step 7   Repeat for each network interface.

Step 8   Restart Windows.

Troubleshooting Service Inventory

lists the troubleshooting steps to perform for Service Inventory.

Table 12-6   *Troubleshooting Checklist for Service Inventory*

	Task	For More Information
Step 1	Check to see that the Cisco Service Inventory service is running.	Services on the Cisco HCM-F Platform, page 3-1
Step 3	Check the Service Inventory alarms located in **activelog syslog/CiscoSyslog**.	Managing Alarms on the Cisco HCM-F Platform, page 12-14 Table 12-10Alarm CLI Commands, page 12-14 For information on individual alarms, see the *Alarm Catalogs for Cisco Hosted Collaboration Mediation Fulfillment.*
Step 4	Check the Service Inventory log files located in: • **activelog tomcat/logs/catalina.out** which includes request and response messages to and from Cisco Unified Communications Domain Manager. • **activelog tomcat/logs/si/log4j** which contains all Service Inventory-specific operations.	Managing Traces on the Cisco HCM-F Platform, page 12-15 Table 12-11Trace CLI Commands, page 12-16

Common Service Inventory Errors

The following section contains common Service Inventory errors.

Service Inventory Job Scheduling Does Not Work—Report Does Not Get Generated

Service Inventory job scheduling does not work as expected, and the report does not get generated.

Service Inventory job scheduling relies on the service provider name for Cisco Unified Communications Domain Manager, which displays in the Infrastructure Manager administrative interface (Service Provider > Administration) and exists in the Shared Data Repository. You can either retrieve the service provider data by using the Cisco HCS CUCDMSync service (strongly recommended) or by manually configuring it in Infrastructure Manager.

Tip   Cisco strongly recommends that you use the Cisco HCS CUCDMSync service so that data configuration get synchronized for Cisco Unified Communications Domain Manager in Cisco HCM-F. If you use the Cisco HCS CUCDMSync service, Service Inventory requires that at least one synchronization has occurred before a report gets generated. If necessary, perform a manual sync after you verify that the Cisco HCS CUCDMSync service is running.

Be aware that if you manually configure the service provider and then activate the Cisco HCS CUCDMSync service, the service overwrites the information that you configure with the information that comes directly from CUCDM.

Perform the following tasks, depending on your configuration:

- Verify the service provider name displays correctly in the Infrastructure Manager administrative interface. In addition, open Cisco Unified Communications Domain Manager and verify that the service provider name for Cisco Unified Communications Domain Manager is correct.

- If the name is correct and you use the Cisco HCS CUCDMSync service, perform troubleshooting tasks for the Cisco HCS CUCDMSync service, as described in the "Troubleshooting Cisco HCS CUCDMSync Service" section on page 12-3.

- If you do not use Cisco HCS CUCDMSync service, update the configuration in the administrative interface. To manually configure the service provider name for CUCDM in the Infrastructure Manager administrative interface, select **Administration > Service Provider**. For manual configuration, configure the Name setting on the Service Provider page in the Infrastructure Manager administrative interface exactly as the service provider name exists on the CUCDM.

Service Inventory Cannot Authenticate to Cisco Unified Communications Domain Manager—Cannot Receive Files

The Service Inventory service encountered a runtime error and cannot validate the request from Cisco Unified Communications Domain Manager; therefore, the Service Inventory service cannot receive the files from Cisco Unified Communications Domain Manager.

Verify that you configured the username and password correctly for Cisco Unified Communications Domain Manager in the Infrastructure Manager administrative interface.

Service Inventory Connection to Cisco Unified Communications Domain Manager Failed—Cannot Retrieve Files

The Service Inventory service encountered a runtime error and cannot connect to the Cisco Unified Communications Domain Manager; therefore, the Service Inventory service cannot receive the files from Cisco Unified Communications Domain Manager.

Perform the following tasks:

- Verify that Cisco Unified Communications Domain Manager is up and running.

- In the Infrastructure Manager administrative interface, verify that you correctly configured the SOAP port for Cisco Unified Communications Domain Manager.

- In the Infrastructure Manager administrative interface, verify that you correctly configured the hostname and IP address for Cisco Unified Communications Domain Manager.

Service Inventory Did Not Receive the Files from Cisco Unified Communications Domain Manager After Time Passed

Service Inventory did not receive the files from Cisco Unified Communications Domain Manager after one hour passed.

Perform the following tasks:

- Log in to Cisco Unified Communications Domain Manager. Select **General Tools > Transactions**. Review the transactions to determine whether the transactions failed.

    - For example, the following message may display in the transaction: "Unhandled exception encountered while performing request processing. Report generation failure. FTP failure. Is there a file of the same name on the FTP server?"

      In the Service Inventory administrative interface, verify that you configured the SFTP port correctly on the Configuration page.

    - For example, the following message may display in the transaction: "Unhandled exception encountered while performing request processing. Report generation failure. FTP failure. Authentication failed."

On the Configuration page in the Service Inventory administrative interface, correct the user credentials for Cisco Unified Communications Domain Manager SFTP access to Service Inventory.

- For example, the following message may display in the translation: "Unhandled exception encountered while performing request processing. Report generation failure. FTP failure. Is there a file of the same name on the FTP server? [Errno -2] Name or service not known."

- Ensure that the Cisco HCM-F platform network connection works as expected.

- If Cisco Unified Communications Domain Manager has DNS enabled, run the **nslookup** command on Cisco Unified Communications Domain Manager to ensure that the Service Inventory hostname resolves.

- If Cisco Unified Communications Domain Manager does not use DNS, verify that you configured the IP address for the Service Inventory server on the Configuration page in the Service Inventory administrative interface.

Service Inventory Received an Empty or Incomplete File from Cisco Unified Communications Domain Manager

Service Inventory received the file from Cisco Unified Communications Domain Manager, but the file is empty or does not contain all data.

In the Infrastructure Manager administrative interface, verify that the Provider configuration matches the configuration that is in Cisco Unified Communications Domain Manager.

The Remote SFTP Server Did Not Receive the Report

The remote SFTP server did not receive the report that Service Inventory transferred.

On the Configuration page in the Service Inventory administrative interface, verify that the remote SFTP server configuration is correct.

Troubleshooting Cisco HCS Platform Manager Service

Table 12-7 on page 12-11 lists the troubleshooting steps to perform for Platform Manager.

Table 12-7   Troubleshooting Checklist for Platform Manager Service

	Task	For More Information
Step 1	Check to see that the Cisco HCS Platform Manager service is running.	Services on the Cisco HCM-F Platform, page 3-1
Step 2	Check for communication problems between the servers.	Configuration Checklist for Platform Manager, page 8-1
Step 3	If you have an issue with an upgrade task, check the server type in the server group. For Upgrade Tasks, publisher server and subscriber servers cannot be in the same group.	Using Server Groups, page 8-4

Table 12-7   Troubleshooting Checklist for Platform Manager Service

	Task	For More Information
Step 4	Check Platform Manager Error Messages.	Common Platform Manager Errors, page 12-12
Step 5	Check the Platform Manager Log Files.	Platform Manager Log Files, page 12-12
		Managing Traces on the Cisco HCM-F Platform, page 12-15
		Table 12-11Trace CLI Commands, page 12-16

Common Platform Manager Errors

The following section contains common Platform Manager errors.

"Could not contact server" or "Server not available"

Make sure the connections between all UC applications and Platform Manager are established before you run a task. All UC applications must be contacted at least once before you run to the first Platform Manager task. SFTP or FTP and UC applications must be routable from the Platform Manager; for example, use public IP if NATs are used. Likewise, the SFTP or FTP servers must be routable from the UC applications.

Platform Manager Log Files

When you troubleshoot issues for Platform Manager, you can access the following log files on the Cisco HCM-F platform at the following locations:

- file get activelog tomcat/logs/platform-api/log4j/*—This log file includes information generated by the UC applications. The same log file is also stored on the application server. Using this command, you can view:
  - SOAP messages from the Platform Manager including inputs, results, errors, and messages
  - Calls to underlying OS components like the upgrade scripts
- file get activelog tomcat/logs/pm/log4j/*—This log file includes information from the Platform Manager. Using this command, you can view:
  - REST traffic between the browser and the Platform Manager including inputs, results, errors, and messages
  - SOAP messages to the UC applications including inputs, results, errors, and messages
  - Database access including updates, queries, and results
  - Task-related events like scheduling, starting, and updating tasks
  - Background jobs like synchronization tasks

Troubleshooting Cisco HCM-F Administrative Interface

Table 12-8 on page 12-13 lists the troubleshooting steps to perform for the Administrative Interface.

Table 12-8   Troubleshooting Checklist for the Administrative Interface

	Task	For More Information
Step 1	Check to see that the following services are running: • Cisco CDM Database • Cisco Tomcat • Cisco HCS Admin UI • Cisco HCS CDM UI • Cisco HCS SI UI • Cisco HCS Service Inventory • Cisco Platform Manager • Cisco HCS vCenter Sync • Cisco HCS CUCDM Sync • Cisco HCS FulFillment	Services on the Cisco HCM-F Platform, page 3-1
Step 2	Check the following log files: • **activelog tomcat/logs/hcsadmin/log4j** • **activelog tomcat/logs/siui/log4j** • **activelog tomcat/logs/cdmui/log4j** • **activelog tomcat/logs/pm/log4j**	Platform Manager Log Files, page 12-12 Managing Traces on the Cisco HCM-F Platform, page 12-15 Table 12-11Trace CLI Commands, page 12-16

Troubleshooting Cisco HCS North Bound Interface Web Service API

Table 12-9 on page 12-13 lists the troubleshooting steps to perform for NBI Web Service API.

Table 12-9   Troubleshooting Checklist for the NBI Web Service API

	Task	For More Information
Step 1	Check to see that the following services are running: • Cisco CDM Database • Cisco JMS Broker • Cisco Tomcat • Cisco HCS Admin UI • Cisco HCS CDM UI • Cisco HCS North Bound Interface Web Service	Services on the Cisco HCM-F Platform, page 3-1
Step 2	Check the log file activelog tomcat/logs/nbi/log4j	Platform Manager Log Files, page 12-12 Managing Traces on the Cisco HCM-F Platform, page 12-15 Table 12-11Trace CLI Commands, page 12-16

Managing Alarms on the Cisco HCM-F Platform

Alarms provide information on runtime status and the state of the system, so you can troubleshoot problems that are associated with your system; for example, to identify issues with the Disaster Recovery System. Alarm information, which includes an explanation and recommended action, also includes the application name, machine name, and so on, to help you perform troubleshooting.

You configure the alarm interface to send alarm information to multiple locations, and each location can have its own alarm event level (from debug to emergency). Alarms can go to the Syslog Viewer (local syslog), Syslog file (remote syslog), SNMP traps, Cisco HCM-SA (Service Assurance), or to all destinations.

When a service issues an alarm, the alarm interface sends the alarm information to the locations that you configure (and that are specified in the routing list in the alarm definition). The system can either forward the alarm information, as is the case with SNMP traps, or the system can write the alarm information to its final destination (such as a log file).

As soon as you enter the CLI command, the system will prompt you for the required parameters. Enter the values to see the output.

Table 12-10 shows the commands that you need to work with alarms on the Cisco HCM-F platform:

Table 12-10   Alarm CLI Commands

Task	Command
Display the alarm configuration for a specific service/list of all services	show alarm Required Parameter: *servicename*—Name of the service. It can contain multiple words. Example: Enter the servicename as *all* to show the alarm configurations of all the services. Enter the servicename as *Cisco Tomcat* to show the alarm configuration of Cisco Tomcat service.
Enable/Disable alarms for a particular destination	set alarm *status* Required Parameters: *status*—enable or disable. *servicename*—Name of the service. It can contain multiple words. *monitorname*—SDI, SDL, Event_Log, or Sys_Log.
Enable alarms for a remote Syslog server	set alarm remotesyslogserver Required Parameters: *servicename*—Name of the service. It can contain multiple words. *servername*—Name of the remote Syslog server.

Table 12-10   Alarm CLI Commands (continued)

Task	Command
Set the event level for an alarm	set alarm *severity* Required Parameters: *servicename*—Name of the service. It can contain multiple words. *monitorname*—SDI, SDL, Event_Log, or Sys_Log. *severity* equals one of the following: – Emergency—This level designates the system as unusable. – Alert—This level indicates that immediate action is needed. – Critical—The system detects a critical condition. – Error—This level signifies that an error condition exists. – Warning—This level indicates that a warning condition is detected. – Notice—This level designates a normal but significant condition. – Informational—This level designates information messages only. – Debug—This level designates detailed event information that Cisco TAC engineers use for debugging.
Set alarm configuration to default values **Tip** This option is available only for service names beginning with Cisco.	set alarm default Required Parameters: *servicename*—Name of the service. It can contain multiple words.

Managing Traces on the Cisco HCM-F Platform

Traces assist you in troubleshooting issues with your application. You use the CLI to specify the level of information that you want traced as well the type of information that you want to be included in each log file. You can configure trace parameters for any service on the Cisco HCM-F platform.

After you have configured information that you want to include in the log files for the various services, you can collect and view log files through log collection. To do this, configure trace using **set trace** CLI command.

You can configure the level of information that you want traced (debug level), what information you want to trace (trace fields), and information about the trace files (such as number of files per service, size of file, and time that the data is stored in the log files)

Configuring Trace

You use the command line interface (CLI) to enable and disable tracing as well as to configure trace settings for specific services on the Cisco HCM-F platform. As soon as you enter the CLI command, the system prompts you for the required parameters. For more information regarding trace collection, see the "Collecting Logs" section on page 12-17.

Table 12-11 shows the commands that you need to work with traces on the Cisco HCM-F platform:

Table 12-11   Trace CLI Commands

Task	Command
Display the trace configuration for a specified service	show trace Required Parameter: *servicename*—Name of the service. It can contain multiple words. Example: Enter the servicename as *all* to show the trace configurations of all the services. Enter the servicename as *Cisco AMC Service* to show the trace configuration of Cisco AMC Service.
Display the trace levels available for a specified service	show tracelevels Required Parameter: *servicename*—Name of the service. It can contain multiple words.
Enable/Disable trace for a specified service	set trace *status* Required Parameters: *status*—enable or disable *servicename*—Name of the service. It can contain multiple words.
Specify the debug trace level settings for a specified service	set trace *tracelevel* Required Parameters: *tracelevel*—Use show tracelevels CLI command to find the trace levels for a given servicename. *servicename*—Name of the service. It can contain multiple words.
Specify the maximum size of a trace files for a specific service from 1 to 10 megabytes.	set trace maxfilesize Required Parameters: *servicename*—Name of the service. It can contain multiple words. *size*—Maximum size of the trace files from 1 to 10 megabytes.

Table 12-11   Trace CLI Commands (continued)

Task	Command
Specify the maximum number of log files per service. The system automatically appends a sequence number to the file name to indicate which file it is; for example, cus299.txt. When the last file in the sequence is full, the trace data begins writing over the first file.	set trace maxnumfiles Required Parameters: *servicename*—Name of the service. It can contain multiple words. *filecount*—Number of trace files from 1 to 10000.
Set the user categories flag to the value provided, for a specified service. **Tip** This option is available only for service names beginning with Cisco.	set trace usercategories Required Parameters: *flagnumber*—Hexadecimal value from 0 to 7FFF. 7FFF means all the flags are enabled. *servicename*—Name of the service. It can contain multiple words.
Set trace configuration to default values for a specified service. **Tip** This option is available only for service names beginning with Cisco.	set trace default Required Parameter: *servicename*—Name of the service. It can contain multiple words.

Collecting Logs

You can collect log files by performing any of the following tasks:

- To view the log files directly from the CLI, enter the following the CLI commands:
    - file list
    - file view
    - file search
- To bundle the various log files and send them to the local SFTP directory, enter the CLI command file get.

    Then, use an SFTP client to obtain the .tar files and send them to the team that troubleshoots.

Use Cisco HCM-SA (Service Assurance) tools to obtain the log files.