Troubleshooting Tools

SNMP on Cisco HCM-F Platform Setup

SNMP version 3 provides security features such as authentication (verifying that the request comes from a genuine source), privacy (encryption of data), authorization (verifying that the user allows the requested operation), and access control (verifying that the user has access to the objects requested). To prevent SNMP packets from being exposed on the network, you can configure encryption with SNMPv3.

The following sections describe how to configure SNMP v3 so the network management system can monitor Cisco HCM-F.

Note To configure SNMP v2, see Enable Sending SNMP v2 Traps from HCM-F, on page 7.

SNMP Configuration

Procedure

Step 1 Install and configure the SNMP NMS.
For more information, refer to the SNMP product documentation that supports the NMS.

Step 2 In the command line interface, enter **utils service list** .
Verify that the system started the SNMP services, including:

- SNMP Master Agent

- System Application Agent
- Cisco Syslog Agent
- MIB2 Agent
- Host Resources Agent

Step 3 Configure the SNMP user.
See
SNMP users, on page 3.

Step 4 Configure the notification destination for traps or informs.
See:

- SNMP trap notification destinations, on page 4
- SNMP Inform notification destination, on page 5

Step 5 Configure the system contact and location for the MIB2 system group.
See MIB2 system group, on page 8.

Step 6 Configure trap settings for CISCO-SYSLOG-MIB.
Use these guidelines to configure CISCO-SYSLOG-MIB trap settings on your system:

- Set clogsNotificationEnabled (1.3.6.1.4.1.9.9.41.1.1.2) to true by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID to true from the linux command line using: snmpset -c <*community string*> -v2c <*transmitter ipaddress*> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1
  You can also use any other SNMP management application for the SNMP Set operation.
- Set clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) value by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID value from the linux command line using: snmpset -c public -v2c 1<*transmitter ipaddress*> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <*value*>
  Enter a severity number for the <value> setting. Severity values increase as severity decreases. A value of 1 (Emergency) indicates highest severity, and a value of 8 (Debug) indicates lowest severity. Syslog agent ignores any messages greater than the value that you specify; for example, to trap all syslog messages, use a value of 8.

Step 7 (Optional) At the command line enter **utils service start SNMP Master Agent** to restart the SNMP Master Agent service.

Tip The system automatically restarts the SNMP Master Agent after you execute the **utils snmp config** command.

Step 8 On the NMS, configure the Cisco HCM-F trap parameters.
For more information refer to:

- SNMP Management Information Base (MIB), on page 9
- SNMP product documentation that supports the NMS

SNMP users

The following table shows the commands for SNMP V3 users on the Cisco HCM-F platform:

Table 1: Trace CLI commands

Task	Command
List the SNMP users.	**utils snmp config 3 user list**
Add an SNMP user.	**utils snmp config 3 user add** The system prompts you for the parameters. See the following table for parameter names and descriptions.
Update an SNMP user.	**utils snmp config 3 user update** The system prompts you for the parameters. See the following table for parameter names and descriptions.
Delete an SNMP user.	**utils snmp config 3 user delete** The system prompts you for the parameters. See the following table for parameter names and descriptions.

The following table describes the SNMP user parameter settings for V3.

Table 2: SNMP user parameter settings for V3

Field	Description
username	The name of the user for which you want to provide access. The name can contain up to 32 characters and can contain any combination of alphanumeric characters, hyphens (-), and underscore characters (_). **Tip** Enter users that you have already configured for the network management system (NMS).
authprotocol	Authentication protocol. To specify HMAC-SHA, enter SHA.
authpassphrase	Specifies the authentication protocol password. The password must contain at least 8 characters.
privprotocol	Specifies the privacy protocol, either AES128, AES192, or AES256
privpassphrase	Specifies the privacy protocol password. The password must contain at least 8 characters.

Field	Description
accessprivilege	Enter one of the following options for the access level: • **ReadOnly—**The user can only read the values of MIB objects. • **ReadWrite—**The user can read and write the values of MIB objects. • **ReadWriteNotify—**The user can read and write the values of MIB objects and send MIB object values for a trap and inform messages. • **NotifyOnly—**The user can only send MIB object values for trap and inform messages. • **ReadNotifyOnly—**The user can read values of MIB objects and also send the values for trap and inform messages. • **None—**The user cannot read, write, or send trap information. **Tip** To change the trap configuration parameters, you need to configure a user with NotifyOnly, ReadNotifyOnly, or ReadWriteNotify privileges.
ipaddress1	Specify an IP address from which to accept packets. The default specifies to accept packets from all hosts.
ipaddress2	Specify the second IP address from which to accept packets. The default specifies to accept packets from all hosts.

SNMP trap notification destinations

An SNMP agent sends notifications to NMS in the form of traps or informs to identify important system events. Traps do not receive acknowledgments from the destination whereas informs do receive acknowledgments.

The following sections apply to SNMP V3 notification destination configuration.

CLI commands for SNMP trap notification destinations

The following table shows the commands for SNMP trap notification destinations on the Cisco HCM-F platform:

Table 3: CLI commands for SNMP trap notification destinations

Task	Command
List trap notification destinations.	**utils snmp config 3 trap list**

Task	Command
Add a v3 trap notification destination that is associated with a configured v3 username.	**utils snmp config 3 trap add** The system prompts you for the parameters. See Trap notification destination parameter settings, on page 5 for parameter names and descriptions.
Update a trap notification destination.	**utils snmp config 3 trap update** The system prompts you for the parameters. See Trap notification destination parameter settings, on page 5 for parameter names and descriptions.
Delete a trap notification destination.	**utils snmp config 3 trap delete** The system prompts you for the parameters. See Trap notification destination parameter settings, on page 5 for parameter names and descriptions.

Trap notification destination parameter settings

The following table describes the trap notification destination parameter settings for V3.

Table 4: Trap notification destination parameter settings for V3

Field	Description
ipaddress	The host IP address of the notification destination.
portno	The notification-receiving port number on the destination server. The default port number is 162.
oldportno	The notification-receiving port number on the destination server that is currently configured.
newportno	The notification-receiving port number on the destination server that you want to use when updating the trap notification destination.
username	Specifies the SNMP user associated to the notification destination.

SNMP Inform notification destination

An SNMP agent sends notifications to NMS in the form of traps or informs to identify important system events. Traps do not receive acknowledgments from the destination whereas informs do receive acknowledgments.

CLI commands for SNMP inform notification destinations

The following table describes the inform notification destination configuration settings for V3.

Table 5: CLI commands for SNMP inform notification destinations

Task	Command
List inform notification destinations.	**utils snmp config 3 inform list**
Add a v3 inform notification destination.	**utils snmp config 3 inform add** The system prompts you for the parameters. See Inform notification destination parameter settings, on page 6 for parameter names and descriptions.
Update an inform notification destination.	**utils snmp config 3 inform update** The system prompts you for the parameters. See Inform notification destination parameter settings, on page 6 for parameter names and descriptions.
Delete an inform notification destination.	**utils snmp config 3 inform delete** The system prompts you for the parameters. See Inform notification destination parameter settings, on page 6 for parameter names and descriptions.

Inform notification destination parameter settings

Table 6: Inform notification destination parameter settings for V3

Field	Description
ipaddress	The host IP address of the notification destination.
portno	The notification-receiving port number on the destination server. The default is port 162.
oldportno	The notification-receiving port number on the destination server that is currently configured.
newportno	The notification-receiving port number on the destination server that you want to use when updating the inform notification destination.
username	Specifies the SNMP user associated to the notification destination.
oldusername	Specifies the v3 username that is currently associated with the inform.
newusername	Specifies the v3 username that you want to associate with the inform.

Field	Description
deleteuserconf	Specifies confirmation for deleting the old user, either Y or N.
authprotocol	Authentication protocol. To specify HMAC-SHA, enter SHA.
authpassphrase	Specifies the authentication protocol password. The password must contain at least 8 characters.
privprotocol	Specifies the privacy protocol, either AES128, AES192, or AES256
privpassphrase	Specifies the privacy protocol password. The password must contain at least 8 characters.
accessprivilege	Enter one of the following options for the access level: • **ReadWriteNotify—**The user can read and write the values of MIB objects and send MIB object values for a trap and inform messages. • **NotifyOnly—**The user can only send MIB object values for trap and inform messages. • **ReadNotifyOnly—**The user can read values of MIB objects and also send the values for trap and inform messages.
engineId	Specifies the remote engine ID of the server to which to send inform messages.

Enable Sending SNMP v2 Traps from HCM-F

Procedure

Step 1 Issue the **utils snmp config 1/2c community-string add** command to add the SNMP v2 community string.
Respond to the prompts:

a) Community string. Enter the community string for HCM-F.
b) Access privilege. Put **ReadWriteNotify**. Note that the default value **ReadOnly** will not enable the trap.
c) Host IP addresses to accept packets from. Agree to the default value **ALLHOSTS**.
d) Agree to restart the SNMP Master Agent.

Step 2 Issue the **utils snmp config 1/2c trap add** command to add the trap destination.
Respond to the prompts:

a) Destination IP address. Enter the IP address of the remote management server.
b) Port number. Agree to the default value 162.
c) SNMP version. Agree to the default value v2c.
d) Community string. Enter the community string for HCM-F.
e) Agree to restart the SNMP Master Agent.

Step 3 Configure the CISCO-SYSLOG-MIB trap setting.

a) As root user, use the **snmpset -c <community string> -v2c <HCM-F IP address> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1** command to set clogsNotificationEnabled to true.

b) As root user, use the **snmpset -c <community string> -v2c <HCM-F IP address> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>** command to set the clogMaxSeverity value.
A value of 1 (Emergency) indicates highest severity, and a value of 8 (Debug) indicates lowest severity. The syslog agent ignores any messages greater than the value that you specify. For example, to trap all syslog messages, use a value of 8.

MIB2 system group

You can use the CLI to configure the system contact and system location objects for the MIB-II system group. For example, you could enter Administrator, 555-121-6633, for the system contact and San Jose, Bldg 23, 2nd floor, for the system location.

MIB2 CLI commands

The following table shows the commands for working with MIB2 system groups on the Cisco IME server:

Table 7: MIB2 CLI commands

Task	Command
List the MIB2 system group configuration.	**utils snmp config mib2 list**
Add a MIB2 system group.	**utils snmp config mib2 add** The system prompts you for the parameters. See CLI parameters for MIB2 system groups, on page 8 for parameter names and descriptions.
Update a MIB2 system group.	**utils snmp config mib2 update** The system prompts you for the parameters. See CLI parameters for MIB2 system groups, on page 8 for parameter names and descriptions.
Delete a MIB2 system group.	**utils snmp config mib2 delete** The system prompts you for the parameters. See CLI parameters for MIB2 system groups, on page 8 for parameter names and descriptions.

CLI parameters for MIB2 system groups

The following table describes the MIB2 system group parameter settings.

Table 8: MIB2 System group parameter settings

Field	Description
Server	The server for which you want to configure contacts.
SysContact	Specifies a person to notify when problems occur.
SysLocation	Specifies the location of the person that is identified as the system contact.

SNMP Management Information Base (MIB)

Simple Network Management Protocol (SNMP) allows access to a Management Information Base (MIB), which is a collection of information that is organized hierarchically. MIBs comprise managed objects, which are identified by object identifiers. A MIB object, which contains specific characteristics of a managed device, comprises one or more object instances (variables).

The SNMP interface provides these Cisco Standard MIBs:

- CISCO-CDP-MIB
- CISCO-SYSLOG-MIB

The SNMP extension agent resides in the server. The SNMP interface also provides these industry-standard MIBs:

- SYSAPPL-MIB
- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB

Cisco HCM-F SNMP Interface supports the following MIBs.

CISCO-CDP-MIB

Use the CDP subagent to read the Cisco Discovery Protocol MIB (CISCO-CDP-MIB). This MIB enables Cisco HCM-F to advertise itself to other Cisco devices on the network.

The CDP subagent implements the CDP-MIB. The CDP-MIB contains the following objects:

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable
- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval

- cdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

SYSAPPL-MIB

Use the System Application Agent to get information from the SYSAPPL-MIB, such as installed applications, application components, and processes that are running on the system.

System Application Agent supports the following object groups of SYSAPPL-MIB:

- sysApplInstallPkg
- sysApplRun
- sysApplMap
- sysApplInstallElmt
- sysApplElmtRun

MIB-II

Use MIB2 agent to get information from MIB-II. The MIB2 agent provides access to variables that are defined in RFC 1213, such as interfaces, IP, and so on, and supports the following groups of objects:

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

HOST-RESOURCES MIB

Use Host Resources Agent to get values from HOST-RESOURCES-MIB. Host Resources Agent provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base. Host Resources Agent supports the following groups of objects:

- hrSystem
- hrStorage

- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

CISCO-SYSLOG-MIB

Syslog tracks and logs all system messages, from informational through critical. With this MIB, network management applications can receive syslog messages as SNMP traps:

Cisco Syslog Agent supports trap functionality with the following MIB objects:

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

Display Diagnostic Reports

Using Infrastructure Manager Administration GUI

Procedure

Step 1 From the Infrastrucute Manager interface, select **Administration** > **Diagnostics**.

Step 2 Select the diagnostic you want from the pulldown menu and click **Request Diagnostics.**

Utils commands

Use the following commands to diagnose problems for Cisco HCS services:

Note The commands shown here are available on an Application Node. A WS Node has a different set. Use the **help utils diagnose hcs** command to display the available commands.

- `utils diagnose hcs`
- `utils diagnose hcs agp`

- `utils diagnose hcs chpa`
- `utils diagnose hcs cnf`
- `utils diagnose hcs cucdmpa`
- `utils diagnose hcs cucdmsync`
- `utils diagnose hcs dmasa`
- `utils diagnose hcs fulfillment`
- `utils diagnose hcs hlm`
- `utils diagnose hcs nbi`
- `utils diagnose hcs sdrcnf`
- `utils diagnose hcs si`
- `utils diagnose hcs ucpa`
- `utils diagnose hcs ucsmsync`
- `utils diagnose hcs usersync`
- `utils diagnose hcs vcentersync`

Troubleshooting with Cisco HCM-F Real-Time Monitoring Tool

Cisco HCM-F Real-Time Monitoring Tool (RTMT), which runs as a client-side application, uses HTTPS to monitor system performance. RTMT has performance counters for Memory, Network, CPU, Disk, Process, and Services including JVM statistics. RTMT can connect directly to devices through HTTPS to troubleshoot system problems.

Launch RTMT

The RTMT application launches when you double click on the application icon or open the application, but does not work properly unless you log in on the proper type of server. In this case, a Cisco Hosted Collaboration Mediation Fulfillment (Cisco HCM-F) server.

You can connect to either the HCM-F application server or the HCM-F Web Services server. The RTMT session does not provide monitoring support for all the servers in HCM-F cluster.

Note You can launch more than one RTMT session, with each session connecting to a different server (for example, one session connection to the HCM-F application server and another session connection to an HCM-F Web Services server). However, multiple RTMT sessions are not recommended by Cisco.

Before You Begin

Ensure that a Cisco CDM Database service is running on the Cisco HCM-F server to which you want to establish the RTMT connection.

Procedure

Step 1 To launch RTMT, perform one of the following tasks:

- On the Windows desktop, double-click the **Real-Time Monitoring Tool** icon.
  Alternatively, select **Start** > **Programs** > **Cisco** > **HCS** > **Real-Time Monitoring Tool**.

  Note If you are working 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**.

- For Linux: If a shortcut does not appear on the desktop, you can use `/opt/Cisco/HCS/JRtmt` to start the RTMT.

The Real-Time Monitoring Tool Login dialog appears.

Step 2 In the Host IP Address field, enter either the IP address or the hostname of the Cisco HCM-F server.

Step 3 Enter the port that the application will use to listen to the server.
The default port is 8443.

Step 4 Check the **Secure Connection** check box.

Step 5 Click **OK**.
If the Add Certificate to Store dialog appears, click **Accept** to continue.

The Authentication Required dialog appears.

Step 6 In the User Name field, enter the Administrator username for the application.

Step 7 In the Password field, enter the password for the Administrator username.
If the authentication fails or if the server is unreachable, RTMT prompts you to reenter the server and authentication details, or you can click **Cancel** to exit the application.

If authentication succeeds, RTMT launches the monitoring module from local cache or from a remote server, if the local cache does not contain a monitoring module that matches the back-end version. The Cisco HCM-F Real-Time Monitoring Tool window and the Select Configuration dialog box appear.

Step 8 Select a profile, and then click **OK**.

Profiles

Add Configuration Profile

With RTMT, you can customize your monitoring window by monitoring different performance counters and then create your own configuration profiles. You can restore these monitoring windows in a single step rather than opening each window again.

You can switch between different profiles during the same RTMT session or use the configuration profile in subsequent RTMT sessions.

Follow this procedure to create a profile.

Procedure

Step 1 Choose **File** > **Profile**.
The Preferences dialog box appears.

Step 2 Click **Save**.
The Save Current Configuration dialog box appears.

Step 3 In the Configuration name field, enter a name for this particular configuration profile.

Step 4 In the Configuration description field, enter a description of this particular configuration profile.

Note Profiles apply to all nodes within a cluster, but you cannot save and apply the profile to a different cluster.

The system creates the new configuration profile.

Restore Configuration Profile

Perform the following procedure to restore a profile that you configured:

Procedure

Step 1 Choose **File** > **Profile**.
The Preferences dialog box appears.

Step 2 Click the profile that you want to restore.

Step 3 Click **Restore**.
All windows with precanned settings or performance monitoring counters for the restored configuration open.

Delete Configuration Profile

Perform the following procedure to delete a profile that you configured:

Procedure

Step 1 Choose **File** > **Profile**.
The Preferences dialog box appears.

Step 2 Click the profile that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Close**.

Alarms management on Cisco HCM-F platform

Alarms provide information about 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 and machine name 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 alarm CLI command, the system prompts you for the required parameters. Enter the values to see the output.

The following table shows the commands for working with alarms on the Cisco HCM-F platform:

Table 9: 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.

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.

Trace management on 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 as the type of information that you want included in each log file. You can configure trace parameters for any service on the Cisco HCM-F platform.

After you configure the information that you want to include in the log files for each service, you can collect and view log files through log collection. To do this, configure trace using the **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).

Trace setup

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 Log collection, on page 18.

The following table shows the commands for working with traces on the Cisco HCM-F platform:

Table 10: 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. You can obtain the name of the service from the **utils service list** CLI command.
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.

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.

Log collection

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.