CHAPTER 19

Troubleshooting

This chapter contains information on the following topics:

- Troubleshooting Tips, page 19-1
- CISCO-CCM-MIB Tips, page 19-2
- HOST-RESOURCES-MIB Tips, page 19-4
- SNMP Developer Tips, page 19-5

Troubleshooting Tips

Review this section for troubleshooting tips:

- Make sure that all the feature and network services that are listed in "SNMP Services" section on page 14-4 are running.
- Verify that the community string or SNMP user is properly configured on the system. You configure the SNMP community string or user by choosing **SNMP > V1/V2 > Community String** or **SNMP > V3> User** in Cisco Unified Serviceability. See "SNMP Configuration Requirements" section on page 14-3 for more information.

Cannot poll any MIBs from the system

This condition means that the community string or the SNMP user is not configured on the system or they do not match with what is configured on the system.

Note By default, no community string or user is configured on the system.

Check whether the community string or SNMP user is properly configured on the system by using the SNMP configuration windows.

Cannot receive any notifications from the system

This condition means that the notification destination is not configured correctly on the system.

Verify that you configured the notification destination properly in the Notification Destination (V1/V2c or V3) Configuration window.

Cannot receive SNMP traps from Cisco Unified Communications Manager node

Verify that you configured the following MIB Object IDentifiers (OIDs) that relate to phone registration/deregistration/failure to the following values (the default for both values equals 0):

- ccmPhoneFailedAlarmInterval (1.3.6.1.4.1. 9.9.156.1.9.2) set to 30-3600. You can use this CLI command: **snmpset -c** <*community string*> **-v2c** <*transmitter ipaddress*> **1.3.6.1.4.1.9.9.156.1.9.2 .0 i <*value*>**
- ccmPhoneStatusUpdateAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.4) set to 30-3600. You can use this CLI command: **snmpset -c** <*community string*> **-v2c** <*transmitter ipaddress*> **1.3.6.1.4.1.9.9.156.1.9.4.0 i <*value*>**

Make sure that all the feature and network services that are listed in "SNMP Services" section on page 14-4 are running.

Verify that you configured the notification destination properly in the Notification Destination (V1/V2c or V3) Configuration window.

Verify that you configured the community string/user privileges correctly, including Notify permissions, in the Community String (V1/V2c) or User (V3) Configuration window.

CISCO-CCM-MIB Tips

Review this section for Cisco CallManager SNMP Service Troubleshooting tips:

- Be sure to set the trace setting to detailed for Cisco CallManager SNMP Service (see SNMP Trace Configuration, page 14-14).
- Execute the command: **snmp walk -c** <*community*> **-v2c** <*ipaddress*> **1.3.6.1.4.1.9.9.156.1.1.2**
- Get the Cisco Unified Communications Manager version details
- Collect the following logs and information:
  - SNMP Master Agent (path: platform/snmp/snmpdm/*) and Cisco CallManager SNMP Service (path: cm/trace/ccmmib/sdi/*) by using TLC in RTMT or this CLI command: **file get activelog**
  - SNMP package version by using this CLI command: **show packages active snmp**
  - MMF Spy output for phone by using this CLI command: **show risdb query phone**
- Send the trace logs and MMFSpy data for further analysis

Table 19-1 provides procedures for verifying that CISCO-CCM-MIB SNMP traps get sent.

Table 19-1 How to Check CISCO-CCM-MIB SNMP Traps

Trap	Verification Procedure
ccmPhoneStatusUpdate	1. Set MaxSeverity=Info in CiscoSyslog->dogBasic MIB table. 2. Set PhoneStatusUpdateAlarmInterv=30 or higher in ccmAlarmConfigInfo MIB table. 3. Disconnect a Cisco Unified CM server that your phones point to. 4. Phones will unregister. 5. Connect the Cisco Unified CM server again. 6. Phones will re-register. 7. Check that the ccmPhoneStatusUpdate trap is generated.
ccmPhoneFailed	1. Set MaxSeverity=Info in CiscoSyslog->clogBasic MIB table. 2. Set PhoneFailedAlarmInterv=30 or higher in ccmAlarmConfigInfo MIB table. 3. Make a phone fail. Delete a phone Cisco Unified Communications Manager Administration and register the phone again. 4. Check that the ccmPhoneFailed trap is generated.
MediaResourceListExhausted	1. Create a Media Resource Group (MRG) that contains one of the standard Conference Bridge resources (CFB-2). 2. Create a Media Resource Group List (MRGL) that contains the MRG just created. 3. In the Phone Configuration window (for actual phones), set MRGL as the phone Media Resource Group List. 4. Stop the IPVMS, which makes the Conference Bridge resource(CFB-2) stop working. 5. If you make conference calls with phones that use the media list, you will see "No Conference Bridge available" in the phone screen. 6. Check that a MediaListExhausted Alarm/Alert/Trap is generated

Table 19-1 How to Check CISCO-CCM-MIB SNMP Traps (continued)

Trap	Verification Procedure
RouteListExhausted	1. Create a Route Group (RG) that contains one gateway. 2. Create a Route Group List (RGL) that contains the RG that was just created. 3. Create a Route Pattern (9.XXXX) that routes a 9XXXX call through the RGL. 4. Unregister the gateway. 5. Dial 9XXXX on one of the phones. 6. Check that a RouteListExhausted Alarm/Alert/Trap is generated.
MaliciousCallFailed	1. Similar to QRT, create a softkey template. In the template, add all available "MaliciousCall" softkey to the phone different status. 2. Assign the new softkey template to actual phones; reset the phones. 3. Make some calls and select the "MaliciousCall" softkey in the phone screen during or after the call. 4. Check that a "MaliciousCallFailed" Alarm/Alert/Trap is generated.

HOST-RESOURCES-MIB Tips

Process Monitoring

HOST-RESOURCES-MIB retrieves information about all the processes that are running on the system from hrSWRunTable. Use the HOST-RESOURCES-MIB when you want to monitor all the processes that are running in the system. To monitor the only the installed Cisco application, use SYSAPPL-MIB.

Memory Usage and RTMT

Table 19-2 maps the memory usage values that are used by RTMT to the HOST-RESOURCES-MIB. Be aware that RTMT and HOST-RESOURCES-MIB use the term "virtual memory" differently.

- The virtual memory that is reported by HOST-RESOURCES-MIB gets reported as swap memory by RTMT.
- The virtual memory that is reported by RTMT equals total memory, or the sum of the physical and swap memory usage.

Because swap memory may return a 0 on low use servers, you can validate this value against the RTMT Memory\Used Swap Kbytes value.

Table 19-2 Mapping RTMT Memory Usage Values to HOST-RESOURCES-MIB

Memory Usage	RTMT Counter	HOST-RESOURCES-MIB
SWAP Memory Usage	Memory\Used Swap Kbytes	hrStorageUsed.2 Equates to Virtual Memory
Physical Memory Usage	Memory\Used Kbytes	hrStorageUsed.1 Equates to Physical RAM
Total Memory (physical + swap) usage	Memory\Used VM Kbytes	Add hrStorageUsed.2 and hrStorageUsed.1 No equivalent description

The hrStorageUsed for physical memory shows the data in terms of used - (buffers + cache).

The shared memory info that is exposed by the MIB follows: HOST-RESOURCES-MIB::hrStorageDescr.10 = STRING: /dev/shm.

For HOST RESOURCES MIB:

%Physical memory usage = (Physical RAM hrStorageUsed + /dev/shm hrStorageUsed) / (Physical RAM hrStorageSize)

%VM used = (Physical RAM hrStorageUsed + /dev/shm hrStorageUsed + Virtual Memory hrStorageUsed) / (Physical RAM hrStorageSize + Virtual Memory hrStorageSize)

Disk Space and RTMT

The used and available disk space values that are shown by HOST-RESOURCES-MIB may not match the disk space values that are shown by RTMT due to the minfree percentage of reserved file system disk blocks. Because the minfree value for Cisco Unified Communications Manager in 6.x and 7.0 systems is 1 percent, you will see a 1 percent difference between the used disk space value that is shown by RTMT and HOST-RESOURCES-MIB.

- In RTMT, the disk space used value gets shown from df reported values: [(Total Space – Available Space) /Total Space] * 100 where the Total Space includes the minfree also.
- For Host Resources MIB, the disk space used value gets calculated by [hrStorageUsed/hrStorageSize] * 100 where the hrStorageSize does not include the minfree.

SNMP Developer Tips

Review this section for SNMP developer troubleshooting tips:

- Refer to the CISCO-CCM-CAPABILITY-MIB at the following link for the support list for CISCO-CCM-MIB:

http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-CCM-CAPABILITY

As stated in the CISCO-CCM-CAPABILITY-MIB, ccmPhoneDevicePoolIndex does not get supported, so it returns a 0. The Callmanager device registration alarm currently does not contain the device pool information.

- If Cisco CallManager SNMP service is not running, only the following tables in the MIB will respond:
  - ccmGroupTable
  - ccmRegionTable
  - ccmRegionPairTable
  - ccmDevicePoolTable
  - ccmProductTypeTable
  - ccmQualityReportAlarmConfigInfo
  - ccmGlobalInfo

  To get Cisco CallManager SNMP service running, activate and start the service in Cisco Unified Serviceability.
- Query the SysApplInstallPkgTable in SYS-APPL MIB to get an inventory of Cisco Unified Communications Manager applications that are installed on the system. Query the SysApplRunTable in SYS-APPL MIB to get an inventory of Cisco Unified Communications Manager applications that are running on the system. Because System Application Agent cannot show services that are activated and deactivated or monitor Web App services or servlets, use this approach to monitor system health and service status for Cisco Unified Communications Manager applications:
  - Use the Serviceability API **getservicestatus** to provide complete status information, including activation status, for both Web applications and non-Web applications. See the *AXL Serviceability API Guide* for more details.
  - Check service status with this CLI command: **utils service list**
  - Monitor the servM-generated messages with Syslog (see the following example):

```
Mar 18 16:40:52 ciscart26 local7 6 : 92: Mar 18 11:10:52.630 UTC :
%CCM_SERVICEMANAGER-SERVICEMANAGER-6-ServiceActivated: Service Activated. Service
Name:Cisco CallManager SNMP Service App ID:Cisco Service Manager Cluster ID: Node
ID:ciscart26
```

Note Cisco Unified Communications Manager uses the following Web application services and servlets: Cisco CallManager Admin, Cisco CallManager Cisco IP Phone Services, Cisco CallManager Personal Directory, Cisco CallManager Serviceability, Cisco CallManager Serviceability RTMT, Cisco Extension Mobility, Cisco Extension Mobility Application, Cisco RTMT Reporter Servlet, Cisco Tomcat Stats Servlet, Cisco Trace Collection Servlet, Cisco AXL Web Service, Cisco Unified Mobile Voice Access Service, Cisco Extension Mobility, Cisco IP Manager Assistant, Cisco WebDialer Web Service, Cisco CAR Web Service, and Cisco Dialed Number Analyzer.

Request Timeout Workaround

If an SNMP request specifies multiple OIDs and the variables are pointing to empty tables, you may get a NO_SUCH_NAME (for SNMP V1) or GENERIC ERROR (for SNMP V2c or V3) due to a timeout problem. A timeout can occur as a result of throttling enhancements to protect the Cisco Unified Communications Manager processing engine.

Note You can retrieve the count of entries in CCMH323DeviceTable and ccmSIPDeviceTable by using scalar objects, so the SNMP Manager (the client) can avoid unnecessary **get/getnext** operations on these tables when no entries exist.

As an SNMP developer, you can use the following workaround for this problem:

- First, use the available scalar variables (1.3.6.1.4.1.9.9.156.1.5) to determine table size before accessing the table or perform the **get** operation on the desired table; then, query the non-empty tables.
- Reduce the number of variables that are queried in a single request; for example, for empty tables, if the management application has the timeout set to 3 seconds, specify only 1 OID. (For non-empty tables, it takes 1 second to retrieve one row of data.)
- Increase the response timeout.
- Reduce the number of retries.
- Avoid using **getbulk** SNMP API. The **getbulk** API retrieves the number of records that is specified by MaxRepetitions, so even if the next object goes outside the table or MIB, it gets those objects. Empty tables cause even more delay. Use **getbulk** API for non-empty tables with a known number of records. In these circumstances, set MaxRepetitions to 5 seconds to require a response within 5 seconds.
- Structure SNMP queries to adapt to existing limits.
- Avoid performing multiple **getbulks** to walk the PhoneTable periodically in case a large number of phones are registered to Cisco CallManager. You can use the ccmPhoneStatusUpdateTable, which updates whenever there is a Phone update, to decide whether to walk the PhoneTable.

Where to Find More Information

Related Topics

- Understanding Services, page 9-1
- Configuring Services, page 11-1
- Understanding Simple Network Management Protocol, page 14-1
- Configuring SNMP V1/V2c, page 15-1
- Configuring SNMP V3, page 16-1
- Configuring SNMP System Group, page 17-1
- Configuring SNMP Trap/Inform Parameters, page 18-1

Related Documentation

Command Line Interface Reference Guide for Cisco Unified Solutions