SNMP Troubleshooting

This chapter provides information for use in SNMP troubleshooting.

Troubleshooting Tips

Review this section for troubleshooting tips:

- Make sure that all the feature and network services that are listed in the SNMP Services section in the *Cisco Unified Serviceability Administration Guide* 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. Refer to *Cisco Unified Serviceability Administration Guide* 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 gets 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

This condition means that you cannot verify SNMP traps from the 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 the SNMP Services section in the *Cisco Unified Serviceability Administration Guide* 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

This section contains tips for CISCO-CCM-MIB.

Related Topics

Frequently Asked Questions, on page 6
General Tips, on page 2
Limitations, on page 5

General Tips

- Be sure to set the trace setting to detailed for Cisco UCM SNMP Service (refer to the *Cisco Unified Serviceability Administration Guide*).
- 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 UCM 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

The following table provides procedures for verifying that CISCO-CCM-MIB SNMP traps get sent.

Table 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 the Cisco Unified Communications Manager server to which your phones register. **4** Phones will unregister. **5** Connect the Cisco Unified Communications Manager 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 from Cisco Unified Communications Manager Administration and register the phone again. **4** Check that the ccmPhoneFailed trap is generated.

Trap	Verification Procedure
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 that was 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" on the phone screen. **6** Check that a MediaListExhausted Alarm/Alert/Trap is generated
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 gets generated.
MaliciousCallFailed	**1** Create a softkey template. In the template, add the "MaliciousCall" softkeys to the different states for the phone. **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 gets generated.

Collect the following logs and information for analysis:

- SNMP Master Agent logs stored at `/platform/snmp/snmpdm/*`.
- Cisco UCM SNMP Service by using the Real Time Monitoring Tool (RTMT) or by entering the **file get activelog** <*path*> CLI command. The path where the logs are stored is */cm/trace/ccmmib/sdi/**.
- All the files in /usr/local/Snmpri/conf folder. (Be aware that this is possible only if ROOT/REMOTE login is available.)
- The 'ls -l' listing of the preceding folder. (Be aware that this is possible only if ROOT/REMOTE login is available.)
- Perfmon logs by executing the **file get activelog /cm/log/ris/csv/** CLI command.
- Details of the set of actions that are performed that resulted in the issue.
- Ccmservice logs by executing the **file get activelog /tomcat/logs/ccmservice/log4j** CLI command.
- SNMP package version by execute the **show packages active snmp** CLI command.
- MMF Spy output for phone by executing the **show risdb query phone** CLI command.

Limitations

If multiple OIDs are specified in the SNMP request and if the variables are pointing to empty tables in CISCO-CCM-MIB, the request takes longer. In case the getbulk/getnext/getmany request has multiple OIDs in its request PDU with the subsequent tables being empty in the CISCO-CCM-MIB, the responses may specify NO_SUCH_NAME for SNMP v1 version or GENERIC_ERROR for SNMP v2c or v3 version.

- Reason—This timeout occurs due to the code that was added to enhance the performance of the CCMAgent and throttle when it gets a large number of queries, thus protecting the priority of Cisco Unified Communications Manager call processing engine.
- Workaround:
    - Use the available scalar variables (1.3.6.1.4.1.9.9.156.1.5) to determine the table size before accessing the table, or do the get operation on the desired table first and then query the nonempty tables.
    - Reduce the number of variables that are queried in a single request. For example, for empty tables. if Management application has timeout set at 3 seconds, Cisco recommends specifying no more than 1 OID. For nonempty tables, it takes 1 second to retrieve 1 row of data.
    - Increase the response timeout.
    - Reduce the number of retries.
    - Avoid using getbulk SNMP API. Getbulk API gets the number of records that is specified by MaxRepetitions. This means that even if the next object goes outside the table or MIB, it gets those objects. So, if the CISCO-CCM -MIB has empty tables, it goes to next MIB and this will need more time to respond. Use getbulk API when you know that the table is not empty and also know the number of records. Under this condition limit the max repetition counts to 5 to get response within 5 seconds.
    - Structure SNMP queries to adapt to current limits.

◦ Avoid doing a number of getbulks on the PhoneTable in case a number of phones are registered to the Cisco Unified Communications Manager. In such a scenario, whenever an update occurs, ccmPhoneStatusUpdateTable gets updated.

Frequently Asked Questions

Why am I not getting any SNMP traps from the Cisco Unified Communication Manager node for the CISCO-CCM-MIB?

For receiving SNMP traps in CISCO-CCM-MIB, you need to ensure that the value of the following MIB OIDs is set to appropriate values: ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) and ccmPhoneStatusUpdateAlarmInterv (1.3.6.1.4.1.9.9.156.1.9.4) are set between 30 and 3600. The default specifies zero (0).

Execute the following commands from any Linux machine:

- **snmpset -c** <*Community String*> **-v 2c** <*transmitter ip address*> **1.3.6.1.4.1.9.9.156.1.9.2.0 i** <*value*>
- **snmpset -c** <*Community String*> **-v 2c** <*transmitter ip address*> **1.3.6.1.4.1.9.9.156.1.9.4.0 i** <*value*>

The Following Issues Relate to Registration, Deregistration, and Failure of Phones

- Configuring notification destinations—You need to ensure that notification destinations are configured. You can do this from the Cisco Unified Serviceability Web window. A menu for **SNMP** > **Notification Destinations** exist.

  Before you configure notification destination, verify that the required SNMP services are activated and running (SNMP Master Agent and Cisco UCM SNMP Services). Also, make sure that you configured the privileges for the community string/user correctly, they should contain Notify permissions as well.

  If traps still are not generated, check whether corresponding alarms are generated. Because these traps get generated based on the alarm events, ensure that SNMP agents are getting these alarm events. Enable Local Syslog. Set up the Cisco UCM Alarm configuration to the informational level for Local Syslog destination from the Alarm configuration that is available on Cisco UCM Serviceability window **Alarm** > **Configuration**. Reproduce the traps and see whether corresponding alarms are logged into the CiscoSyslog file.

- Receiving syslog messages as traps—To receive syslog messages above a particular severity as traps, set the following 2 MIB objects in the clogBasic table:

  - clogNotificationsEnabled (1.3.6.1.4.1.9.9.41.1.1.2)—Set this to **true** (**1**) to enable syslog trap notification. Default value specifies **false** (**2**). For example, **snmpset -c** <*Community String*> **-v 2c** <*transmitter ip address*> **1.3.6.1.4.1.9.9.41.1.1.2.0 i** <*value*>.
  - clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3)—Set the severity level above which traps are desired. Default value specifies **warning** (**5**). All syslog messages with alarm severity lesser than or equal to configured severity level get sent as traps if notification is enabled. For example, **snmpset -c** <*Community String*> **-v 2c** <*transmitter ip address*> **1.3.6.1.4.1.9.9.41.1.1.3.0 i** <*value*>

What are the different traps that are defined for Cisco Unified Communication Manager?

The CISCO-CCM-MIB contains the following list of defined traps:

- ccmCallManagerFailed—Indication that the Cisco UCM process detects a failure in one of its critical subsystems. It can also get detected from a heartbeat/event monitoring process.
- ccmPhoneFailed—Notification that the intervals that are specified in ccmPhoneFailedAlarmInterval indicate at least one entry in the ccmPhoneFailedTable.
- ccmPhoneStatusUpdate—Notification that gets generated at the intervals specified in ccmPhoneStatusUpdateInterv if there one entry in the ccmPhoneStatusUpdateTable exists.
- ccmGatewayFailed—Indication that at least one gateway attempted to register or communicate with the Cisco UCM and failed.
- ccmMediaResourceListExhausted—Indication that Cisco UCM has run out of a specified type of resource.
- ccmRouteListExhausted—Indication that the Cisco UCM could not find an available route in the indicated route list.
- ccmGatewayLayer2Change—Indication that the D-Channel/Layer 2 of a registered interface in a skinny gateway changes state.
- ccmMaliciousCall—Indication that a user registers a call as malicious with the local Cisco UCM server.
- ccmQualityReport—Indication that a user reports a quality problem using the Quality Report Tool.
- ccmTLSConnectionFailure—Indication that the Cisco Unified Communications Manager failed to open TLS connection for the indicated device.

The mapping of the traps to alarms follows:

- ccmCallManagerFailed—CallManagerFailure
- ccmPhoneFailed—DeviceTransientConnection
- ccmPhoneStatusUpdate
- ccmGatewayFailed—DeviceTransientConnection
- ccmMaliciousCall—MaliciousCall
- ccmMediaResourceListExhausted—MediaResourceListExhausted
- ccmQualityReportRequest—QRTRequest
- ccmRouteListExhausted—RouteListExhausted
- ccmGatewayLayer2Change—DChannelOOS, DChannelISV

How can different SNMP traps from Cisco Unified Communication Manager be checked?

Use the following procedure for triggering few traps:

- ccmPhoneStatusUpdate trap
  - Set ccmPhoneStatusUpdateAlarmInterv (1.3.6.1.4.1.9.9.156.1.9.4) to 30 or higher in ccmAlarmConfigInfo MIB table.
  - Disconnect the Cisco Unified Communications Manager server where your phones are registered. Phones will unregister.
  - Connect the Cisco Unified Communications Manager server again. Phones will re-register and you will get the ccmPhoneStatusUpdate trap.

- ccmPhoneFailed trap
  - Set ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) to 30 or higher in ccmAlarmConfigInfo MIB table.
  - Make a phone fail. Delete a phone from Cisco Unified Communications Manager and register the phone again. For phone failed traps, you can try two different scenarios:

    Set the phone to point to tftp/Cisco Unified Communications Manager server A. Plug the phone into Cisco Unified Communications Manager server B on different switch. The phone status remains unknown. You will see following message:

    ```
    2007-10-31:2007-10-31 14:53:40 Local7.Debug 172.19.240.221
    community=public, enterprise=1.3.6.1.4.1.9.9.156.2.0.2,
    enterprise_mib_name=ccmPhoneFailed, uptime=7988879,
    agent_ip=128.107.143.68, version=Ver2, ccmAlarmSeverity=error,
    ccmPhoneFailures=1.
    ```

    Register a 7960 phone as a 7940 phone in the Cisco UCM and cause the db issue that generates the phone fail trap.

- MediaResourceListExhausted trap
  - Create a Media Resource Group (MRG) and have it contain one of the standard ConferenceBridge resources (CFB-2).
  - Create a Media Resource Group List (MRGL) and have it contain the MRG just created.
  - In the Phone Configuration window for real phones, set MRGL as the phone Media Resource Group List.
  - Stop the IPVMS, which makes the ConferenceBridge resource (CFB-2) stop working.
  - Make conference calls with phones by using the media list; you will see No Conference Bridge available on the phone screen.
  - Check whether a MediaListExhausted alarm/alert/trap gets generated.

- RouteListExhausted trap
  - Create a Route Group (RG) and have it contain one gateway.
  - Create a Route Group List (RGL) and have it contain the RG just created.
  - Create a Route Pattern (9.XXXX) that reroutes a 9XXXX call through the RGL.
  - Unregister the gateway.
  - Dial 9XXXX on one of the phones.
  - Check whether a RouteListExhausted alarm/alert/trap gets generated.

- MaliciousCallFailed trap
  - Create a softkey template. In the template, add all available MaliciousCall softkeys to the phone status.
  - Assign the new softkey template to real phones; reset the phones.
  - Make calls and select the MaliciousCall in the phone screen during or after the call.

- Check whether a MaliciousCallFailed alarm/alert/trap gets generated.

- GatewayFailed trap
  - Method 1: Remove the gateway configuration from the database by using Web Admin or change the gateway MAC address to an invalid value and update. Reboot the gateway. Or restart the Cisco UCM service to which the gateway is connected.
  - Method 2: Set GatewayAlarmEnable=true in ccmAlarmConfigInfo MIB table. In Cisco Unified Serviceability, go to the SNMP configuration window to ensure that you have the SNMP community string and trap destination set correctly. Create a gateway failure event and the trap gets displayed on the trap receiver. To cause a gateway failure and failover, restart Cisco UCM. The gateway fails over to the redundant Cisco UCM server. The gateway should not be configured in the database on the redundant Cisco UCM server.

- ccmGatewayLayer2Change trap
  - ccmGatewayLayer2Change trap gets triggered during D-Channel Out of service (DChannelOOS) or D-Channel Inservice (DChannelISV) from Cisco UCM. Check whether any such events gets triggered for testing purposes.

- ccmCallManagerFailed trap
  - The Cisco UCM failed alarm gets generated when an internal error occurs. These alarms include an internal thread dying due to lack of CPU, timer issues, and other issues. This trap would represents something that is hard to reproduce unless the Cisco UCM team intentionally causes one of these occurrences.

If the Cisco UCM Agent consumes high CPU continuously, what needs to be done?

Collect logs for analysis and refer to defect CSCsm74316. Verify whether the defect fix was added to your Cisco UCM release.

If the CTI Routepoint is deleted from Cisco Unified Communications Manager Administration, an entry exists for that in ccmCTIDeviceTable mib. Why?

A service parameter that is called “RIS Unused Cisco CallManager Device Store Period” defines how long unregistered devices remain in RIS database and in the MIB. The Cisco UCM Administration window and the SNMP MIB may not be in sync because the Cisco UCM Administration window shows information from the database and SNMP uses the RIS database.

When ccmPhoneType is queried from ccmPhoneTable in Cisco-CCM-MIB, no information is returned. Why?

This means that the ccmPhoneType has been obsoleted. You can retrieve the same information from ccmPhoneProductTypeIndex against CcmProductTypeEntry. In the table, the indexes correspond to the index and name as listed in that table.

The following list gives some of other obsolete and alternate OIDs to be referred:

- Because ccmGatewayType is obsolete, you need to refer to ccmGateWayProductTypeIndex.
- Because ccmMediaDeviceType is obsolete, you need to refer to ccmMediaDeviceProductTypeIndex.
- Because ccmCTIDeviceType is obsolete, you need to refer to ccmCTIDeviceProductTypeIndex.

A query on ccmPhoneProductTypeIndex returns zero. Why?

Verify that the Cisco Unified Communications Manager release that you are using has this capability.

While a WALK is performed on ccmPhoneTable, ccmPhoneUserName is not returning any value. How are usernames associated to the IP phones?

Create an end user and go to the phone that has been registered and associate the Owner User ID. After this is done, the OID in the SNMP Walk will show the user.

How do I get the firmware versions of each phone by using SNMP?

ccmPhoneLoadID object in the ccmPhoneTable will give the firmware version of each phone. This value may differ if new image download failed because SNMP exposes both configured firmware ID (ccmPhoneLoadID) and the actual running firmware (ccmPhoneActiveLoad).

CCM MIB returns ccmVersion as 5.0.1, which is incorrect.

Verify the Cisco Unified Communications Manager release that you are using has this capability. If it does not, upgrade.

CCM MIB returns incorrect ccmPhoneLoadID

ccmPhoneLoadID values get picked up from the RIS database, which gets populated based on the alarm that is received during phone registration. Perform the following steps and collect the logs for further analysis:

1. In Cisco Unified Serviceability, choose **Alarm** > **Configuration**. Choose the server; then, click **Go**. Choose **CM Services** for the Services Group; then, click **Go**. Choose **Cisco CallManager** for the service; then, click **Go**.
2. Check **Enable Alarm** for Local Syslog, SDI Trace, and SDL Trace. Choose **Informational** from each Alarm Event Level drop-down list box.
3. In the Trace Configuration window, set the Debug Trace Level for the Cisco UCM service to **Detailed**.
4. Reset the phones that are showing incorrect LoadID.
5. Collect the Syslog and Cisco UCM traces.
6. Collect the phone details.

How Cisco Call Manager status (START/STOP) monitored?

For service monitoring, you have following options:

- SYSAPPL MIB
- HOST-RESOURCE-MIB
- CISCO-CCM-MIB (ccmStatus)
- SOAP interface
- Real-Time Monitoring Tool (RTMT) alerts

A ccmCallManagerFailed trap exists for Cisco UCM service failures. But this does not cover normal service stop and unknown crashes.

Why does the device pool information seem incorrect for any device that was polled? The OID that was used is ccmPhoneDevicePoolIndex.

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

HOST-RESOURCES-MIB Tips

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 only the installed Cisco application, use SYSAPPL-MIB.

Related Topics

Disk Space and RTMT, on page 11
Frequently Asked Questions, on page 12
Logs for Collection, on page 11

Logs for Collection

Collect the following logs and information for troubleshooting purposes:

- The hostagt log files by executing the **file get activelog /platform/snmp/hostagt/** command.
- The syslog files by executing the **file get activelog /syslog/** command.
- Master SNMP Agent log files by executing the **file get activelog /platform/snmp/snmpdm/** command.
- Sequence of operations performed.

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 Release 7.1(x) and later systems equals 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.

Frequently Asked Questions

Can the HOST-RESOURCES-MIB be used for process monitoring?

Host resources MIB does retrieve the information about the processes that are running on the system in hrSwRunTable; however, this monitors all the processes that are running in the system. If you need to monitor only the installed Cisco Application, the best way requires you to use SYSAPPL-MIB.

How are the memory usage values that are shown by Real-Time Monitor Tool mapped to the HOST-RESOURCES-MIB?

The following table lists the memory usage values.

Table 2: Memory Usage Values

Memory Usages	RTMT Counter	HOST-RESOURCES-MIB
SWAP memory Usage	Memory\Used Swap Kbytes	hrStorageUsed.2 (whose description is virtual memory)
Physical Memory Usage	Memory\Used Kbytes	hrStorageUsed.1(whose description is Physical RAM)
Total memory (physical + swap) usage	Memory\Used VM Kbytes	No equivalent. Basically need to add hrStorageUsed.2 and hrStorageUsed.1 Because you cannot use swap memory at all on lightly used servers, HR Virtual Memory may return 0. To validate HR VM is returning correctly, you need to compare the value against RTMT Memory\Used Swap KBytes. RTMT and HR use the term "Virtual memory" differently. The hrStorageUsed for physical memory shows the data in terms of used - (buffers + cache). The hrStorageUsed for physical memory shows the data in terms of used that is buffers + cache. The shared memory information that is exposed by the HOST-RESOURCES-MIB is ::hrStorageDescr.10 = STRING: /dev/shm. The virtual memory that gets reported by HOST-RESOURCES-MIB comprises what is considered as swap memory by RTMT. For HOST RESOURCES MIB, the following formula gets used: • %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)

Why do the disk space values shown by RTMT and the HOST-RESOURCES-MIB differ?

In general, the df size will not match the used and available disk space data shown. This occurs because of minfree percentage of reserved filesystem disk blocks. The minfree value for a Cisco Unified Communication Manager in Releases 6.x and 7.0 is 1percent. The difference of 1 percent occurs between the disk space used value that is shown in 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 the HOST-RESOURCES-MIB, this gets calculated by [hrStorageUsed/hrStorageSize] * 100 wherein the hrStorageSize does not include the minfree.

How does the Host Agent display the value in hrStorageUsed?

The hrStorageUsed for physical RAM got corrected to show the data in terms of used (buffers + cache). To check whether the host agent version is correct, collect the snmp-rpm version that is installed in the system by using the **show packages active snmp** command.

How the Memory Capacity/Usage Values compare to those of HOST-RESOURCES-MIB?

In the HOST-RESOURCES-MIB, the size and storage used get represented in terms of hrStorageUnits. If, for that storage type, the hrStorageUnits equals 4096 bytes, the hrStorageUsed or hrStorageSize value queried in the MIB value should get multiplied by 4096. For example, by using the **show status** command, the Total Memory displays as 4090068K for Physical RAM.

If the hrStorageUnits for physicalRAM storage type equals 4096 bytes, the hrStorageSize for Physical RAM will get shown as 1022517, which is 4090078K [(1022517 x 4096)/1024 = 4090068K].

Why does an SNMP query on hrSWRunName in HOST-RESOURCES-MIB intermittently return incorrect entries in Windows?

The Microsoft SNMP extension agent (hostmib.dll) supports the HOST-RESOURCE-MIB. Microsoft support may be able to help on this. If the problem is persistent, perform the following steps:

1. Use the tlist snmp.exe file to verify that the hostmib.dll is listed in the output.
2. Verify that no error/warning messages from SNMP exist in the event viewer when SNMP service is started.
3. Make sure that the community string used has been configured with read privilege under snmp service properties.
4. Use MSSQL-MIB (MssqlSrvInfoTable) to confirm SQL process status.

Monitoring Processes

HOST-RESOURCES-MIB retrieves information about all the processes that are running on the system from hrSWRunTable. Use this MIB for monitoring all the processes that are running in the system. To monitor only the installed Cisco application, use SYSAPPL-MIB.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 equals 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.

CISCO-CDP-MIB Tips

This section contains the following topics:

Related Topics

Frequently Asked Questions, on page 14
General Tips, on page 14

General Tips

Collect the following logs and information for analysis:

- Use the **set trace enable Detailed cdpmib** command to set the detailed trace for cdpAgt ().
- Restart the Cisco CDP Agent service from the Cisco Unified Serviceability window (**Tools** > **Control Center** > **Network Services**) and wait for some time.
- Collect the following trace files:
  - Enable the Cisco CDP Agent traces by using the **file get activelog cm/trace/cdpmib/sdi** command and Cisco CDP daemon traces by using the **file get activelog cm/trace/cdp/sdi** command.
  - Enable the Cisco CDP Agent and daemon traces by using the Real-Time Monitoring Tool (RTMT) **Trace & Log Central** > **Collect Files** > **Cisco CallManager SNMP Service** > **Cisco CDP Agent and Cisco CDP**.
- After the logs are collected, reset the trace setting by using the **set trace disable cdpmib** command.

Frequently Asked Questions

Why are the CDP interface table and globalinfo tables are blank?

Verify that your Cisco UCM release has this capability. If not, upgrade.

How is the MessageInterval value set in the Interface table as well as Global table in CDP MIB?

Check to see whether the HoldTime value is greater than MessageInterval value. If it is less, the MessageInterval value cannot get set from both interface table and global table.

SYSAPP-MIB Tips

This section contains tips for SYSAPP-MIB.

Related Topics

Collecting Logs, on page 15
Using Servlets in Cisco Unified Communications Manager 8.0, on page 15

Collecting Logs

Collect the following logs and information for analysis. Execute the command **file get activelog** *<paths in the following bullets>*

- SNMP Master Agent Path: `/platform/snmp/snmpdm/*`
- System Application Agent Path: `/platform/snmp/sappagt/*`

Using Servlets in Cisco Unified Communications Manager 8.0

The SysAppl MIB provides a way to get inventory of what is installed and running at a given time. SysAppl agent cannot give the list of services that are activated or deactivated. It can only provide the running/not running states of the application/services. Web App services/Servlets cannot get monitored by using the SysAppl MIB. The following servlets exist for a 8.0 system:

- Cisco CallManager Admin
- Cisco CallManager Cisco IP Phone Services
- Cisco CallManager Personal Directory
- Cisco CallManager Serviceability
- Cisco CallManager Serviceability RTMT
- Cisco Dialed Number Analyzer
- 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
- Cisco Dialed Number Analyzer

For monitoring important service status for system health purposes, Cisco recommends the following approaches:

- Use the Cisco Unified Serviceability API that is called GetServiceStatus. This API can provide complete status information, including activation status for both web application type and non web app services. (See *AXL Serviceability API Guide* for more details.)
- Use the **utils service list** command to check the status of different services.
- Use the Syslog message and monitor the servM generated messages. For 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
```

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

  CISCO-CCM-CAPABILITY

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

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

    To get Cisco UCM 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 Cisco Unified Serviceability API that is called 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 UCM Admin, Cisco UCM Cisco IP Phone Services, Cisco UCM Personal Directory, Cisco Unified Serviceability, Cisco Unified RTMT, Cisco Extension Mobility, Cisco Extension Mobility Application, Cisco Unified 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 UCM. 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 Documentation

- *Command Line Interface Reference Guide for Cisco Unified Solutions*
- "SNMP" chapter, *Cisco Unified Serviceability Administration Guide*