Simple Network Management Protocol

Simple Network Management Protocol support

SNMP basics

Simple Network Management Protocol (SNMP), an application layer protocol, facilitates the exchange of management information among network devices, such as nodes, routers, and so on. As part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.

You use Cisco Unified IM and Presence Serviceability to configure SNMP-associated settings, such as community strings, users, and notification destinations for V1, V2c, and V3. Likewise, in the SNMP configuration windows, you can apply the settings to all nodes in the cluster.

An SNMP-managed network comprises of three key components: managed devices, agents, and network management systems.

- Managed device—A network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.

  The first node in the IM and Presence cluster acts as the managed device.

- Agent—A network-managed software module that resides on a managed device. An agent contains local knowledge of management information and translates it into a form that is compatible with SNMP.

  IM and Presence uses a master agent and subagent components to support SNMP. The master agent acts as the agent protocol engine and performs the authentication, authorization, access control, and privacy functions that relate to SNMP requests. Likewise, the master agent contains a few Management Information Base (MIB) variables that relate to MIB-II. The master agent also connects and disconnects subagents after the subagent completes necessary tasks. The SNMP master agent listens on port 161 and forwards SNMP packets for Vendor MIBs.

The IM and Presence subagent interacts with the local IM and Presence only. The IM and Presence subagents send trap and information messages to the SNMP Master Agent, and the SNMP Master Agent communicates with the SNMP trap receiver (notification destination).

- Network Management System (NMS)—A SNMP management application (together with the PC on which it runs) that provides the bulk of the processing and memory resources that are required for network management. An NMS executes applications that monitor and control managed devices. IM and Presence works with the following NMS:
    - Cisco Unified Operations Manager
    - HP OpenView
    - Third-party applications that support SNMP and IM and Presence SNMP interfaces

SNMP version 1 support

SNMP version 1 (SNMPv1), the initial implementation of SNMP that functions within the specifications of the Structure of Management Information (SMI), operates over protocols, such as User Datagram Protocol (UDP) and Internet Protocol (IP).

The SNMPv1 SMI defines highly structured tables (MIBs) that are used to group the instances of a tabular object (that is, an object that contains multiple variables). Tables contain zero or more rows, which are indexed, so SNMP can retrieve or alter an entire row with a supported command.

With SNMPv1, the NMS issues a request, and managed devices return responses. Agents use the Trap operation to asynchronously inform the NMS of a significant event.

In Cisco Unified IM and Presence Serviceability, you configure SNMP v1 support in the **V1/V2c Configuration** window.

Related Topics

SNMP V1/V2c setup

SNMP version 2c support

As with SNMPv1, SNMPv2c functions within the specifications of the Structure of Management Information (SMI). MIB modules contain definitions of interrelated managed objects. The operations that are used in SNMPv1 are similar to those that are used in SNMPv2. The SNMPv2 Trap operation, for example, serves the same function as that used in SNMPv1, but it uses a different message format and replaces the SNMPv1 Trap.

The Inform operation in SNMPv2c allows one NMS to send trap information to another NMS and to then receive a response from the NMS.

In Cisco Unified IM and Presence Serviceability, you configure SNMP v2c support in the **V1/V2c Configuration** window.

Related Topics

SNMP V1/V2c setup

SNMP version 3 support

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.

Instead of using community strings like SNMP v1 and v2, SNMP v3 uses SNMP users.

In Cisco Unified IM and Presence Serviceability, you configure SNMP v3 support in the **V3 Configuration** window.

Related Topics

SNMP V3 setup
SNMP community strings and users, on page 3

SNMP services

To support SNMP, you must use the following services, which display in the **Control Center-Network Services** screen in Cisco Unified IM and Presence Serviceability.

- SNMP Master Agent
- MIB2 Agent
- Host Resources Agent
- System Application Agent
- Native Agent Adaptor
- Cisco CDP Agent
- Cisco Syslog Agent

Caution Stopping any SNMP service may result in loss of data because the network management system no longer monitors the Cisco Unified Communications Manager network. Do not stop the services unless your technical support team tells you to do so.

Related Topics

Feature and network services

SNMP community strings and users

Although SNMP community strings provide no security, they authenticate access to MIB objects and function as embedded passwords. You configure SNMP community strings for SNMP v1 and v2c only.

SNMP v3 does not use community strings. Instead, version 3 uses SNMP users. These users serve the same purpose as community strings, but users provide security because you can configure encryption or authentication for them.

In Cisco Unified IM and Presence Serviceability, no default community string or user exists.

Related Topics

SNMP V1/V2c setup
SNMP V3 setup

SNMP traps and informs

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. You configure the notification destinations by using the **SNMP Notification Destination Configuration** windows in Cisco Unified IM and Presence Serviceability.

For SNMP notifications, traps are sent immediately if the corresponding trap flags are enabled. In the case of the syslog agent, the alarms and system level log messages are sent to syslog daemon for logging. Also, some standard third-party applications send the log messages to syslog daemon for logging. These log messages are logged locally in the syslog files and are also converted into SNMP traps/notifications.

The “Syslog message generated” SNMP trap/inform message is sent to a configured trap destination.

Tip Before you configure notification destination, verify that the required SNMP services are active and running. Also, make sure that you configured the privileges for the community string/user correctly.

Tip You configure the SNMP trap destination by selecting **SNMP** > **V1/V2** > **Notification Destination** or **SNMP** > **V3** > **Notification Destination** in Cisco Unified IM and Presence Serviceability.

The following table provides information about IM and Presence trap/inform parameters that you configure on the Network Management System (NMS). You can configure the values in the table below by issuing the appropriate commands on the NMS, as described in the SNMP product documentation that supports the NMS.

Note Be aware that the parameters that are listed in the table below are part of CISCO-SYSLOG-MIB.

Table 1: IM and Presence Trap/Inform Configuration Parameters

Parameter Name	Default Value	Generated Traps	Configuration Recommendations
clogNotificationsEnabled	False	clogMessageGenerated	To enable trap generation, set clogNotificationsEnable to True.

Parameter Name	Default Value	Generated Traps	Configuration Recommendations
clogMaxSeverity	Warning	clogMessageGenerated	When you set clogMaxSeverity to warning, a SNMP trap generates when IM and Presence applications generate a syslog message with at least a warning severity level.

SNMP Management Information Base (MIB)

SNMP allows access to 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 Simple Network Management Protocol (SNMP) extension agent resides in each IM and Presence node. IM and Presence supports the following MIBs.

CISCO-CDP-MIB

Use the IM and Presence CDP subagent to read the Cisco Discovery Protocol MIB, CISCO-CDP-MIB. This MIB enables IM and Presence 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:

- sysApplInstalled
- sysApplRun
- sysApplMap

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. The Host Resources Agent provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base. The Host Resources Agent supports the following groups of objects:

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

CISCO-SYSLOG-MIB

The system supports trap functionality only. The Cisco Syslog Agent supports only the following objects of CISCO-SYSLOG-MIB:

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

Vendor-Specific MIBs

The following MIBs exist on various Cisco MCS, depending on vendor and model number. To query these MIBS, you can use the standard MIB browsers that are developed by the hardware vendors; for example, HP Systems Insight Manager (SIM) and IBM Director Server+Console. For information about using the MIB browsers, refer to the documentation that the hardware vendor provides.

To review the vendor-specific MIB information, see the following tables:

Table 2: IBM MIBs

MIB	OID	Description
Supported for browsing only		
IBM-SYSTEM-HEALTH-MIB	1.3.6.1.4.1.2.6.159.1.1.30	Provides temperature, voltage, and fan status
IBM-SYSTEM-ASSETID-MIB	1.3.6.1.4.1.2.6.159.1.1.60	Provides hardware component asset data
IBM-SYSTEM-LMSENSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.80	Provides temperature, voltage, and fan details
IBM-SYSTEM-NETWORK-MIB	1.3.6.1.4.1.2.6.159.1.1.110	Provides Network Interface Card (NIC) status
IBM-SYSTEM-MEMORY-MIB	1.3.6.1.4.1.2.6.159.1.1.120	Provides physical memory details
IBM-SYSTEM-POWER-MIB	1.3.6.1.4.1.2.6.159.1.1.130	Provides power supply details
IBM-SYSTEM-PROCESSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.140	Provides CPU asset/status data
Supported for system traps		
IBM-SYSTEM-TRAP	1.3.6.1.4.1.2.6.159.1.1.0	Provides temperature, voltage, fan, disk, NIC, memory, power supply, and CPU details
IBM-SYSTEM-RAID-MIB	1.3.6.1.4.1.2.6.167.2	Provides RAID status

Table 3: HP MIBs

MIB	OID	Description
Supported for browsing and system traps		
CPQSTDEQ-MIB	1.3.6.1.4.1.232.1	Provides hardware component configuration data

MIB	OID	Description
CPQSINFO-MIB	1.3.6.1.4.1.232.2	Provides hardware component asset data
CPQIDA-MIB	1.3.6.1.4.1.232.3	Provides RAID status/events
CPQHLTH-MIB	1.3.6.1.4.1.232.6	Provides hardware components status/events
CPQSTSYS-MIB	1.3.6.1.4.1.232.8	Provides storage (disk) systems status/events
CPQSM2-MIB	1.3.6.1.4.1.232.9	Provides iLO status/events
CPQTHRSH-MIB	1.3.6.1.4.1.232.10	Provides alarm threshold management
CPQHOST-MIB	1.3.6.1.4.1.232.11	Provides operating system information
CPQIDE-MIB	1.3.6.1.4.1.232.14	Provides IDE (CD-ROM) drive status/events
CPQNIC-MIB	1.3.6.1.4.1.232.18	Provides Network Interface Card (NIC) status/events

Set up SNMP

The following procedure provides the tasks for configuring SNMP.

See the SNMP product documentation that supports the NMS for more information.

Procedure

Step 1 Install and configure the SNMP NMS.

Step 2 In the **Control Center—Network Services** window, verify that the system started the SNMP services.

Step 3 If you are using SNMP v3, configure the SNMP user.

Step 4 Configure the notification destination for traps or informs.

Step 5 Configure the system contact and location for the MIB2 system group.

Step 6 Restart the Master Agent service.

Step 7 On the NMS, configure the Cisco Unified Communications Manager trap parameters.

Related Topics

- Configure a community string
- Configure a notification destination for SNMP V1/V2c
- Configure a notification destination for SNMP V3
- Configure an SNMP user
- Configure the MIB2 system group
- Feature and network services in Cisco Unified Serviceability
- SNMP services, on page 3
- SNMP traps and informs, on page 4

Troubleshooting SNMP

Review this section for troubleshooting tips. Make sure that all of the feature and network services are running.

Problem

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

Solution

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

Problem

Cannot receive any notifications from the system

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

Solution

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

Related Topics

- SNMP services, on page 3