CHAPTER 26

Configuring SNMP

Configuring SNMP is optional for the Cisco TelePresence Exchange System. At minimum, however, Cisco recommends that you configure SNMP on the administration servers to monitor the entire system via the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB. This product-specific MIB enables you to monitor all nodes in the Cisco TelePresence Exchange System server cluster as well as all resources that you configure on the Cisco TelePresence Exchange System. With this product-specific MIB, the remote management system needs to monitor or query only one of the administration servers to determine the status of each resource and cluster node.

If you also want to monitor the hardware and operating system (such as the server memory, CPU, disk usage, power supplies, and fans) of each server, configure SNMP on all nodes in the Cisco TelePresence Exchange System server cluster.

Note Cisco recommends that SNMP clients use a 5-second or longer timeout when querying the Cisco TelePresence Exchange System.

This chapter includes the following sections:

Restrictions for SNMP

- SNMP version 1 is not supported. Only SNMP versions 2c and 3 are supported.
- SNMP inform requests are not supported. SNMP notifications are sent as traps only.
- SNMP configurations are not replicated between servers. Whenever you change the SNMP configuration, whether via the CLI or via SNMP Set operations to read-write objects, you must manually apply the same configuration changes to each of the other servers.
- The CISCO-SYSLOG-MIB is implemented and will respond to queries, but the syslog messages are currently unformatted and raw.

- The Cisco TelePresence Exchange System supports MIB persistence on indexes and read-write objects of the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB. The system automatically saves the indexes and read-write set operations every four hours, starting at midnight (0000) UTC.
  - If you set an object, then wait four hours before restarting the SNMP service or rebooting the server. Otherwise, the object may be set to its previous value after the SNMP service restart.
  - If you configure an SNMP-monitored item (such as a media resource) via the Cisco TelePresence Exchange System administration console, CLI, or API, then wait four hours before restarting the SNMP service or rebooting the server. Otherwise, the item you added may not remain indexed as it was before the SNMP service restart.
  - Indexes are not reused. If you configure an SNMP-monitored item and then remove it, the index for that item will be void. If you add the item back again, the item will get a new index.

For additional details about the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB, see the "CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB" section on page D-1.

Supported MIBs

The CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB was created specifically to manage the Cisco TelePresence Exchange System. This MIB is implemented only on the administration servers, but it manages all six nodes in the server cluster and monitors all resources that are configured on the Cisco TelePresence Exchange System.

Other RFC-based MIBs are also supported and may be implemented on all Cisco TelePresence Exchange System servers to provide hardware and operating system information, for example, about the CPU, memory, power supplies, and fans. IBM servers implement the IBM MIBs.

For a complete list of supported MIBs, see the *MIBs Supported by Cisco TelePresence Exchange System* document at ftp://ftp.cisco.com/pub/mibs/supportlists/CTXSystem/CTXSystem-supportlist.htm.

Related Topics

- CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB, page D-1
- Resource Monitoring, page 26-3

About SNMP on the Cisco TelePresence Exchange System

See the following sections:

- Cluster Node Monitoring, page 26-3
- Resource Monitoring, page 26-3
- Trap Flood Mitigation, page 26-3

Cluster Node Monitoring

Each administration server independently queries each node in the Cisco TelePresence Exchange System server on a 30-second interval by running one of the following commands, depending on the node role:

- utils service adminserver status
- utils service database status
- utils service sipserver status

The status returned from each query is updated in the ctxClusterNodeTable, and you can view the status as the operational state in the System > Cluster Nodes area of the administration console.

Resource Monitoring

The Cisco TelePresence Exchange System monitors the resources that are configured in the system on a fixed interval. Table 26-1 shows how and when each resource type is monitored.

Note The system does not monitor the following resources:

- Any resources that are configured to be in the maintenance state in the Cisco TelePresence Exchange System.
- Resources that are not configured in the Cisco TelePresence Exchange System, such as the Cisco TelePresence Video Communication Server.

Table 26-1 Resource Monitoring Intervals and Methods

Resource Type	Resource Examples	Probe Interval	Probe Methods
SIP-based resources	• Cisco Session Border Controller • Cisco TelePresence Multipoint Switch • Cisco router with IVR[1] • Cisco TelePresence ISDN GW MSE 8321	15 seconds	SIP OPTIONS PING
XML-RPC–based resources	• Cisco TelePresence Server 7010 • Cisco TelePresence MCU MSE 8510	15 seconds	SIP OPTIONS PING and XML-RPC PING
Cisco TelePresence Manager		5 seconds	API PING

1. IVR = Integrated Voice Response

Trap Flood Mitigation

As a rate-limiting feature, traps are sent at 5-second intervals. Specifically, instead of generating and sending a trap as soon as each event is received, the system collects events for up to 5 seconds and then generates traps on the fifth second.

Most of the traps are stateful, meaning that they have an *inAlarm* trap and a *clearing* trap. Using a stateful trap ensures that additional events for the same issue are not sent more than once, unless the trap was cleared first.

How to Configure SNMP

Which tasks you must complete, and on which servers you complete those tasks, depend on the extent of your SNMP implementation.

To	Do This
(Strongly recommended) Use the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB to obtain Cisco TelePresence Exchange System–specific information about the entire server cluster and configured resources.	Complete these tasks on both administration servers: • Adding SNMP Users, page 26-4 • Adding SNMP Trap Destinations, page 26-6 • Adding a Cluster-Identifying VIP Address to SNMP Notifications, page 26-8 • Enabling or Disabling Traps from the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB, page 26-10
(Recommended) Monitor the server-specific hardware and operating system, such as the memory, CPU, disk usage, power supplies, and fans.	Complete these tasks on all six Cisco TelePresence Exchange System servers: • Adding SNMP Users, page 26-4 • Adding SNMP Trap Destinations, page 26-6
Remove SNMP configurations.	• Deleting an SNMP User, page 26-5 • Removing an SNMP Trap Destination, page 26-7 • Removing the Cluster-Identifying VIP Address from SNMP Notifications, page 26-10
Troubleshoot SNMP issues.	• Troubleshooting SNMP, page 26-12

Adding SNMP Users

Complete this procedure on each Cisco TelePresence Exchange System server on which you want to enable SNMP queries.

Before You Begin

- For each server on which you complete this task, make sure that you use the exact same configuration on the other server of the same node role.
- You can add up to ten SNMP users on each server.
- For details about any command or its options, see Appendix C, "Command Reference."
- If you are not sure whether to complete this task, or on which server to complete it, see the "How to Configure SNMP" section on page 26-4.

Procedure

Step 1 Log in to the CLI of the server.

Step 2 Enter one of the following commands, depending on whether you use SNMP version 3 or version 2c:

- **set snmp user add 3** *username* {**r** | **w** | **rw**} [**authNoPriv** | **authPriv** | **authNoPriv**] *passphrase*
- **set snmp user add 2c** *community-string* {**r** | **w** | **rw**}

Note If you use both SNMP versions 3 and 2c, make sure that no version 3 usernames are the same as any version 2c community strings.

Examples:

```
admin: set snmp user add 3 mrtg rw authNoPriv tstpwd
Successfully added user
admin: set snmp user add 2c public r
Successfully added user
```

Step 3 To verify the SNMP user addition, enter the **show snmp users** command.

```
admin: show snmp users
1)  Username: mrtg                      Version: v3
       Level: AuthNoPriv                   Mode: RW

2) Community: public                    Version: v2c
       Level: n/a                          Mode: R
```

You should also now be able to query the Cisco TelePresence Exchange System server on which you added the SNMP user.

Step 4 Repeat this procedure on the other applicable nodes in the Cisco TelePresence Exchange System server cluster.

What to Do Next

Proceed to the "Adding SNMP Trap Destinations" section on page 26-6.

Deleting an SNMP User

Before You Begin

For details about any command or its options, see Appendix C, "Command Reference."

Procedure

Step 1 Log in to the CLI of the server.

Step 2 To display the configured SNMP users, enter **show snmp users**.

```
admin: show snmp users
1)  Username: mrtg                      Version: v3
       Level: AuthNoPriv                   Mode: RW

2) Community: public                    Version: v2c
       Level: n/a                          Mode: R
```

```
3)  Username: testuser                  Version: v3
       Level: AuthNoPriv                   Mode: RW
```

Step 3 Enter one of the following commands, depending on whether you use SNMP version 3 or version 2c:

- **set snmp user del 3** *username*
- **set snmp user del 2c** *community-string*

Example:

```
admin: set snmp user del 3 testuser
Successfully deleted user
```

Step 4 To verify the SNMP user deletion, enter the **show snmp users** command.

```
admin: show snmp users
1)  Username: mrtg                      Version: v3
       Level: AuthNoPriv                   Mode: RW

2) Community: public                    Version: v2c
       Level: n/a                          Mode: R
```

Adding SNMP Trap Destinations

Complete this procedure on each Cisco TelePresence Exchange System server from which you want to receive trap notifications.

Before You Begin

- For each server on which you complete this task, make sure that you use the exact same configuration on the other server of the same node role.
- You can add up to five trap destinations on each server.
- For details about any command or its options, see Appendix C, "Command Reference."
- If you are not sure whether to complete this task, or on which server to complete it, see the "How to Configure SNMP" section on page 26-4.

Procedure

Step 1 Log in to the CLI of the server.

Step 2 Enter one of the following commands, depending on whether you use SNMP version 3 or version 2c:

- **set snmp trapdest add 3** *username destination*[**:***port*] [*level*] *passphrase* [*engineID*]
- **set snmp trapdest add 2c** *community-string destination*[**:***port*] [*passphrase*]

The *destination* is the IP address or hostname of the host where you want the Cisco TelePresence Exchange System to send trap notifications.

For the *level*, specify **authNoPriv**, **authPriv**, or **noauthNoPriv**.

Step 3 To verify the trap destination addition, enter the **show snmp trapdests** command.

```
admin: show snmp trapdests
  1) Host = 192.0.2.162 (Version 2c)
```

```
   Version 2c Options:
      Community = public
```

Step 4 Repeat this procedure on the other applicable nodes in the Cisco TelePresence Exchange System server cluster.

What to Do Next

If you want to identify redundant product-specific notifications from the same Cisco TelePresence Exchange System server cluster, proceed to the "Adding a Cluster-Identifying VIP Address to SNMP Notifications" section on page 26-8.

Removing an SNMP Trap Destination

Procedure

Step 1 Log in to the CLI of the server.

Step 2 Enter **set snmp trapdest del**.

```
admin: set snmp trapdest del
  1) Host = 10.101.180.49:162 (Version 3)

     Version 3 Options:
            User = TimTrap               PW   = authpriv
           Level = authnopriv            Hash = md5
        EngineID = 0x80001f8803001a6406bc16

  2) Host = 10.101.180.49 (Version 3)

     Version 3 Options:
            User = TimTrap2              PW   = authpriv
           Level = authnopriv            Hash = md5
        EngineID = 0x80001f8803001a6406bc16

  3) Host = 10.101.180.49:162 (Version 3)

     Version 3 Options:
            User = trapusr               PW   = trappass
           Level = authnopriv            Hash = md5
        EngineID = 0x8000DEECAFE8111BEEFADE
```

Step 3 When prompted, enter the number from the displayed list to specify the trap destination to delete.

```
  Enter which trap number to delete: 2
Successfully deleted trap destination
```

Step 4 Enter the **show snmp trapdests** command and verify that the deleted trap destination no longer appears.

```
admin: show snmp trapdests
  1) Host = 10.101.180.49:162 (Version 3)

     Version 3 Options:
            User = TimTrap               PW   = authpriv
           Level = authnopriv            Hash = md5
        EngineID = 0x80001f8803001a6406bc16

  2) Host = 10.101.180.49:162 (Version 3)
```

```
Version 3 Options:
       User = trapusr               PW   = trappass
      Level = authnopriv            Hash = md5
   EngineID = 0x8000DEECAFE8111BEEFADE
```

Adding a Cluster-Identifying VIP Address to SNMP Notifications

Product-specific notifications about the Cisco TelePresence Exchange System are sent from the two administration servers via the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB. Because both of the administration servers are active, the system may send redundant SNMP notifications.

To help you identify redundant product-specific notifications from the same Cisco TelePresence Exchange System server cluster, you can configure the administration servers to add an SNMP object called "SNMP-COMMUNITY-MIB::snmpTrapAddress" to the VarBind list of each trap that is generated by the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB.

The snmpTrapAddress value specifies a virtual IP (VIP) address that your remote management system can associate with a specific Cisco TelePresence Exchange System server cluster. You can configure one of the following VIP addresses as the snmpTrapAddress value:

- (Recommended) VIP address of the call engine servers as configured on the SIP load balancer, which is the Cisco Application Control Engine (ACE).
- SNMP (UDP port 161) VIP address that you configure on the ACE to enable it to act as a load-balanced reverse proxy to the administration servers. Specifically, configure an SNMP server farm on the ACE as a reverse proxy where one administration server is a real server (rserver), while the second administration server is a standby rserver.

  If you choose this option, all SNMP Get and Set operations to the administration server SNMP VIP address will go only to the administration server that you configured as the rserver. If the rserver goes down, the Get and Set operations will go only to the administration server that you configured as the standby rserver.

  Note Cisco does not recommend using this SNMP VIP address to monitor the hardware and operating system for the administration servers. If you do so, you will monitor only one of the two administration servers for the cluster. To monitor the hardware or operating system of any Cisco TelePresence Exchange System server, Cisco recommends that you use the IP address of the specific server.

- VIP address to identify both administration servers in the cluster. This VIP address is not required for installation and is not configured anywhere else on the Cisco TelePresence Exchange System.

When two product-specific notifications include the same snmpTrapAddress value, then you know that they were sent from the same Cisco TelePresence Exchange System server cluster. The source IP address of each trap packet identifies the administration server that sent the notification.

Note In each SNMP trap that is sent by any node in the Cisco TelePresence Exchange System server cluster, the source IP address identifies which node sent the trap. If you complete the procedure below, the SNMP-COMMUNITY-MIB::snmpTrapAddress object will be added only to notifications from the administration servers that are generated by the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB.

Before You Begin

- If you complete this task, make sure that you use the exact same configuration on both administration servers in the cluster.
- Complete the procedure in the "Adding SNMP Trap Destinations" section on page 26-6.
- Import the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB into your network management server or SNMP monitoring package.

  To download the MIB, go to:
  ftp://ftp.cisco.com/pub/mibs/v2/CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB.my

Procedure

Step 1 Log in to the CLI of the administration server.

Step 2 Enter **set adminserver trapvip ena** *vip-address*, specifying the VIP address to use as the snmpTrapAddress value that your remote management system can associate with the Cisco TelePresence Exchange System server cluster:

```
admin: set adminserver trapvip ena 10.22.128.212
Updated SNMP Trap VIP to 10.22.128.212
```

Step 3 To verify the configuration, enter **show trapvip**.

```
admin: show trapvip
SNMP Trap VIP: 10.22.128.212
```

Step 4 Repeat this procedure for the second administration server in the cluster.

Examples

The following example shows a received trap *without* the snmpTrapAddress VarBind:

```
TRAP: UDP: [10.21.79.129]:60482 (. 0.0)
    sysUpTimeInstance = Timeticks: (45688631) 5 days, 6:54:46.31
    snmpTrapOID.0 = OID: ciscoCTXSysSystemBackupStatusChg
    ctxSystemBackupStatus.0 = INTEGER: normal(1)
    ctxNotifyMessage.2 = STRING: 2010-10-28T02:49:10.021Z Backup Status OK Cause:
StartTime:2010-10-18T00:00:00.000Z
```

The following example shows a received trap *with* the snmpTrapAddress VarBind:

```
TRAP: UDP: [10.21.79.129]:60482 (. 0.0)
    sysUpTimeInstance = Timeticks: (45688631) 5 days, 6:54:46.31
    snmpTrapOID.0 = OID: ciscoCTXSysSystemBackupStatusChg
    snmpTrapAddress.0 = IpAddress: 10.22.128.212
    ctxSystemBackupStatus.0 = INTEGER: normal(1)
    ctxNotifyMessage.2 = STRING: 2010-10-28T02:49:10.021Z Backup Status OK Cause:
StartTime:2010-10-18T00:00:00.000Z
```

What to Do Next

(Optional) If you want to disable any of the traps that are sent by the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB, proceed to the "Enabling or Disabling Traps from the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB" section on page 26-10.

Removing the Cluster-Identifying VIP Address from SNMP Notifications

Before You Begin

If you complete this task, make sure that you do so on both administration servers in the cluster.

Procedure

Step 1 Log in to the CLI of the administration server.

Step 2 Enter **set adminserver trapvip dis**.

```
admin: set adminserver trapvip dis
Disabled SNMP Trap VIP
```

Step 3 To verify the configuration, enter **show trapvip**.

```
admin: show trapvip
SNMP Trap VIP is not enabled/configured on this server.
```

Step 4 Repeat this procedure for the second administration server in the cluster.

Related Topics

- Adding a Cluster-Identifying VIP Address to SNMP Notifications, page 26-8

Enabling or Disabling Traps from the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB

To control whether or not the system sends specific notifications that are offered by the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB, you can use SNMP Set operations on the objects under the ctxNotifyConfigObjects subtree.

Note

- The SNMP user must have read-write access to use SNMP Set operations.
- SNMP configurations are not replicated between Cisco TelePresence Exchange System servers. If you change the value of any read-write objects on one administration server, you must manually implement the same change on the other administration server.

For objects that are set to true, the notifications that are controlled by those objects will be enabled. For objects that are set to false, the notifications that are controlled by those objects will be disabled.

Use SNMP Get operations to check the values of these objects.

The CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB offers the following notifications:

- ciscoCTXSysAdminServersStatusChg
- ciscoCTXSysDatabaseServersStatusChg
- ciscoCTXSysCallEnginesStatusChg
- ciscoCTXSysResourceStatusChg
- ciscoCTXSysSystemConfigStatusChg

- ciscoCTXSysSystemBackupStatusChg
- ciscoCTXSysLicenseFailure
- ciscoCTXSysUserAuthFailure
- ciscoCTXSysClusterNodeDown
- ciscoCTXSysClusterNodeUp
- ciscoCTXSysResourceDown
- ciscoCTXSysResourceUp
- ciscoCTXSysResourceAllocFailure
- ciscoCTXSysCallSetupFailure
- ciscoCTXSysCallAbnormalDisconnect
- ciscoCTXSysErrorHistoryEvent

Example

Suppose that you do not want the system to send ciscoCTXSysUserAuthFailure notifications. Open the MIB file and find the notification description, which states which object in the ctxNotifyConfigObjects subtree controls whether or not the notification is sent:

```
ciscoCTXSysUserAuthFailure NOTIFICATION-TYPE
    OBJECTS         { ctxNotifyMessage }
    STATUS          current
    DESCRIPTION
        "This notification will be sent when a user authentication
        failure results in CTX System.
           1. User authentication errors while trying to log into
              the CTX System Admin UI.
           2. User authentication errors while trying to log into
              the CTX System CLI.

        ctxAuthFailureNotifyEnable controls whether this notification
        is sent or not."
   ::= { ciscoTelepresenceExchangeSystemMIBNotifs 8 }
```

In the MIB file, find the object description, which includes the following information:

- Which notifications the object controls—an object may control more than one notification.
- Default value of the object—true (notifications are enabled) or false (notifications are disabled).

For example:

```
ctxAuthFailureNotifyEnable OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "This object specifies if the authentication failure traps
        should be enabled or disabled. Setting this to TRUE
        will enable the notifications.  Setting this to FALSE
        will disable the notifications.

        The default setting for authentication failures is
        FALSE/disabled in order to prevent unnecessary event
        flooding.

        This object controls the generation of the following
        notifications:
```

```
        ciscoCTXSysUserAuthFailure"
DEFVAL          { false }
::= { ctxNotifyConfigObjects 3 }
```

Using your preferred method and tools, use SNMP Get operations to view the current value of the ctxAuthFailureNotifyEnable object in the ctxNotifyConfigObjects subtree.

If you want to change the value, use SNMP Set operations to do so on both administration servers.

Related Topics

- CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB, page D-1
- Restrictions for SNMP, page 26-1

Troubleshooting SNMP

- You can use the **utils snmp get** and **utils snmp walk** commands to troubleshoot SNMP from within the Cisco TelePresence Exchange System.
- If a product-specific notification is not being sent as expected, see the "Enabling or Disabling Traps from the CISCO-TELEPRESENCE-EXCHANGE-SYSTEM-MIB" section on page 26-10.