Configure Cisco Emergency Responder Serviceability

- Cisco Emergency Responder Serviceability Configuration Overview , on page 1
- Serviceability Tools , on page 1
- SNMP Configuration , on page 3
- System Monitor Tools , on page 5
- Use Emergency Responder Logs , on page 7

Cisco Emergency Responder Serviceability Configuration Overview

Note The following information addresses SNMP Management. For information about SNMP setting for phone tracking , refer to Set Up SNMP Connection.

Emergency Responder supports SNMP V1/V2C and V3. You can use the Serviceability web interface to configure SNMP V1/V2C (Community String and Notification Destination) and SNMP V3 (User and Notification Destination).

Each SNMP version has security models and security levels. Users are assigned to groups that are defined by a security model and specified security levels. Each group also has a defined security access level to a set of MIB objects for reading and writing, which are known as views. The switch has a default view (all MIB objects) and defaults groups defined for SNMP V1 and V2C security models. SNMP V3 provides additional security features that cover message integrity, authentication, and encryption. In addition, SNMP V3 controls user access to specific areas of the MIB tree.

The following sections describe how to configure SNMP V1/V2C and V3.

Serviceability Tools

The following sections describe the Emergency Responder Serviceability tools.

Use Control Center

The Control Center allows you to perform actions on the services running on the selected Emergency Responder system.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **Tools > Control Center**.
The Control Center page appears.

Step 2 To change the status of a service, click the radio button to the left of the Service Name and click the button corresponding to the desired action. Available actions are:

- Start
- Stop
- Restart

Note Cisco Tomcat and Cisco IDS services cannot be started, stopped, or restarted from the Emergency Responder Serviceability website. These services can only be started, stopped, or restarted using the CLI.

Step 3 Click **Refresh** to refresh the page.

Related Topics

Control Center

Use Event Viewer

The Event Viewer allows you to view events for the prior six months.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **Tools > Event Viewer**.
The Event Viewer page appears.

Step 2 Click **Find** without entering any search criteria to find all events that occurred over the prior six months

To find events that match specific criteria, enter search criteria:

- Select a specific month to view events from the month only.
- If you select Type, you can then select the type on which to search from the pull-down menu to the right.

If you select Module, you can then select the module on which to search from the pull-down menu to the right.

Note For a list of available Types and Modules, see Event Viewer.

When you have entered your search criteria, click **Find**.

Step 3 Perform an ascending or descending sort of the results. To perform a sort, click the up arrow or down arrow next to the Time, Type, or Module column headings.

Related Topics

Event Viewer

SNMP Configuration

Note The following SNMP configuration information is for SNMP management. For information on SNMP setting for phone tracking, see Set Up SNMP Connection.

Emergency Responder supports SNMP V1/V2C and V3. You can use the Serviceability web interface to configure SNMP V1/V2C (Community String and Notification Destination) and SNMP V3 (User and Notification Destination).

Each SNMP version has security models and security levels. Users are assigned to groups that are defined by a security model and specified security levels. Each group also has a defined security access level to a set of MIB objects for reading and writing, which are known as views. The switch has a default view (all MIB objects) and defaults groups defined for SNMP V1 and V2C security models. SNMP V3 provides additional security features that cover message integrity, authentication, and encryption. In addition, SNMP V3 controls user access to specific areas of the MIB tree.

The following sections describe how to configure SNMP V1/V2C and V3.

Set Up SNMP Community String

By configuring SNMP, you can control SNMP access to the Emergency Responder SNMP agent. A management station must first submit a valid community string for authentication.

You configure a community string by entering the Community String Name, the IP addresses of host that can be authenticated using the community string, and the access privileges allowed. The available access privileges are as follows:

- ReadOnly
- ReadWrite
- ReadWriteNotify
- NotifyOnly
- None

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **SNMP > V1/V2C Configuration > Community String**.
The SNMP Community String Configuration page appears.

Step 2 Enter the name of the community string in the Community String Name text box.

Step 3 Click **Accept SNMP Packets only from these hosts** to specify specific hosts whose SNMP packets will be accepted, enter the IP addresses in the text box, and click **Insert**.

To accept SNMP packets from any host, click the **Accept SNMP Packets from any host** radio button.

Step 4 Select the host IP address and click **Remove** to remove an existing host, .

Step 5 Select the access privilege for the host from the Access Privileges pull-down menu then click **Insert**.

Related Topics

SNMP Community String Configuration

Set Up SNMP Users

SNMP V3 provides additional security features that include message integrity, authentication, and encryption. In addition, SNMP V3 controls user access to specific areas of the MIB tree.

Note FIPS Mode and Enhanced Security Mode do not support MD5 or DES encryption methods. If SNMPv3 setting is enabled using MD5 or DES, then enabling FIPS Mode or Enhanced Security Mode changes these encryption methods to SHA-1 or AES-128 respectively.

Before Emergency Responder (in FIPS Mode) upgrade, ensure that there are no MD5 or DES encryption methods in the FIPS Mode. If the MD5 or DES encryption methods were not updated to SHA-1 or AES-128 respectively in the FIPS Mode before upgrade, they will get updated automatically after the upgrade.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, choose **SNMP** > **V3 Configuration** > **User**.

Step 2 Click **Add New** to add a new SNMP User.

Step 3 Enter the new SNMP user name in the **User Name** text box.

Step 4 Check the **Authentication Required** check box to require authentication. Enter a password in the **Password** text box, reenter the password in the **Reenter Password** textbox, and choose either **MD5** or **SHA** to select an authentication protocol. Click **Insert** to add the user.

Step 5 Check the **Privacy Required** check box to require information privacy. Enter a password in the **Password** textbox, reenter the password in the **Reenter Password** textbox, and choose either **DES** or **AES** to select a privacy protocol.

Note A message appears to restart the SNMP master agent for the changes to take effect. Click **OK** to restart the SNMP master agent or **Cancel** to continue without restarting the master agent.

The new user is added to the list of users on the SNMP User Configuration page.

Step 6 Repeat Step 2 through to Step 4 to add additional users.

Related Topics

SNMP User Configuration

Set Up MIB2

The SNMP MIB2 tool allows you to specify a contact person for a MIB2 managed node and the physical location of the managed node.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **SNMP > System Group Configuration > MIB2 System Group Configuration**.

Step 2 In the **System Contact** text box, enter the name of the contact.

Step 3 In the **Location** text box, enter the location of the managed node.

Step 4 Click **Update** in the upper left corner of the page.

Step 5 Click **Clear** in the upper left corner of the page to modify the information, enter the new information in the **System Contact** and **Location** text boxes, and click **Update**.

Related Topics

MIB2 System Group Configuration

System Monitor Tools

The following sections describe how to use the System Monitor tools.

Use CPU and Memory Usage Tool

You can use the CPU and Memory Usage tool to monitor and log this information. By default, the information is refreshed every 30 seconds. You change how often the information refreshes, or you can disable the auto-refresh feature.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **System Monitor > CPU & Memory Usage**.

The CPU and Memory Usage page appears.

The page is divided into two sections **Processors** and **Memory**. For details about the information that is displayed, see Table 1.

Step 2 Enter a value (in seconds) in the **Set the screen refresh value** text box to change the rate at which the page refreshes, and click **Set**. The minimum value you can enter is 5 seconds.

Step 3 Check the **Disable Auto-Refresh** check box in the upper left corner to disable the auto-refresh feature.

Step 4 Click the **Start Log** button in the Processors section of the page to create a log file of the CPU usage.

Click **Start Log** in the Memory section of the page to create a log file of the Memory usage.

You can create up to 25 log files.

The default interval for logging is 10 seconds. To change the logging interval, follow these steps:

a) To change the CPU logging interval, enter a value between 5 seconds and 600 seconds in the **Set CPU Logging Interval** text box and click **Set**.
b) To change the Memory logging interval, enter a value between 5 seconds and 600 seconds in the **Set Memory Logging Interval** text box and click **Set**.

Step 5 Click **Download CPU Log File** or **Download Memory Log File** to download the log files.

The system displays a Log Files page that shows all the current log files. Thereafter, log files are recycled; when a new log file is added, the oldest log file is deleted.

Step 6 To download individual files, click the check box to the left of the log file names that you want to download. To download all log files, check the check box to the left of the File Name column heading. When you have selected the files, click **Download**. If you select multiple files for download, the system creates and downloads a zipped folder called CPULogs (for Processor log files) and MemoryLogs (for Memory log files).

Step 7 To view the log files online without downloading them, click the file name. The system displays the contents of the log file.

Related Topics

CPU and Memory Usage

Use Processes Tool

You can use the Processes tool to monitor and log process information. By default, the information is refreshed every 30 seconds; the minimum refresh value is 5 seconds. You can change how often the information refreshes, or you can disable the auto-refresh feature.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **System Monitor > Processes**.

The Processes page appears. For details about the information that is displayed, see Table 2.

You can perform an ascending or descending sort of the results. To perform a sort, click the up arrow or down arrow next to the column heading that you want to sort by. For example, to perform a descending sort based on the process, click the down arrow next to the Process column heading. Similarly, to perform an ascending sort based on the process ID, click the up arrow next to the PID column heading.

Step 2 Enter a value in the **Set the screen refresh value** text box in the upper right corner and click **Set** to change the rate at which the page refreshes. The minimum value you can enter is 5 seconds.

Step 3 Select the **Disable Auto-Refresh** check box in the upper left corner to disable the auto-refresh feature.

Step 4 Select the check box to the left of the process name and click **View Selected Processes** to view the details of a process. You can select a maximum of ten processes.

The Selected Processes displays the details of the process. On this page you can also set the refresh rate and disable the auto-refresh feature. To start a log of the process, click **Start Log**. To stop a log, click **Stop Log**.

To change the Process logging interval, enter a value between 5 seconds and 600 seconds in the **Set Process Logging Interval** text box and click **Set**.

Step 5 Click **Download Process Logs** from the Process Log Files page to download the log files. To download log files click **Download Log File** from the Processes page.

Step 6 Select the check box to the left of the log file names to download individual files. To download all log files, click the check box to the left of the File Name column heading. When you have selected the files, click **Download**. If you select multiple files for download, the system creates and downloads a zipped folder called ProcessLogs.

Step 7 You can also view the log files online without downloading them. To do so, click the file name. The system displays the contents of the log file in a separate window.

Related Topics

Processes

Use Disk Usage Tool

The Disk Usage tool displays the percentage of available disk space used by the different partitions in the system.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **System Monitor > Disk Usage**.

The Disk Usage page appears. For details about the Disk Usage page, see Table 1.

Step 2 Perform an ascending or descending sort. Click the up arrow or down arrow next to the column heading that you want to sort by. For example, to perform a descending sort based on the partition, click the down arrow next to the Partition column heading. Similarly, to perform an ascending sort based on the available disk space, click the up arrow next to the Available Space column heading.

Related Topics

Disk Usage

Use Emergency Responder Logs

Emergency Responder provides an interface to collect system and application logs. These logs share the same user interface and log files can be viewed and downloaded in the same manner. The following procedure applies to all of the Emergency Responder logs.

Emergency Responder logs are organized into three types. The three types, and the logs within these types, are as follows:

- CER Logs
  - CER Admin
  - CER Server
  - CER Phone Tracking
  - JTAPI

- Tomcat
- Event Viewer
- Audio Driver

- Platform Logs
  - CLI
  - CLM
  - Certificate Management/IPSec
  - DRS
  - Install/Upgrade
  - Remote Support
  - Syslog
  - Servm

- DB Logs
  - Cerdbmon
  - Install DB

- CLI Output Files
  - Platform
  - DB

- SLM Logs
  - SLM
  - GCH
  - TP

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **System Logs > Log Type > Log Name**.

The selected Log Files page appears. See Use Emergency Responder Logs , on page 7 for details about each of these page.

You can perform an ascending or descending sort of the results. To perform a sort, click the up arrow or down arrow next to the column heading that you want to sort by.

Step 2 Download the log files to your local system using the **Download** button.

To select individual files, click the check box to the left of the log file name you want to download. To select all log files, click the check box to the left of the File Name column heading. When you have selected the files, click **Download**. If you select multiple files for download, the system creates and downloads a zipped folder called CPULogs. The names of the zipped folders are based on the type of logs they contain, as follows:

- CER Admin
- CERr Server
- CER Phone Tracking
- Syslog
- JTAPI
- Tomcat
- Install
- DRS
- CLILogs
- CMILogs
- ServmLogs
- RemoteSupportLogs
- InstallDBLogs
- CertificateManagement&IPSecLogs
- CerdbmonLogs
- CLIOutputPlatform
- CLIOutputDB
- SLMLogs
- GCHLogs
- TPLogs

Step 3 Click the file name to view the log files online without downloading them.
The system displays the contents of the log file in a separate window.

Step 4 Click **Reload Log File** to refresh the log file you are viewing.

Step 5 Click **Download Log** to download the log file you are viewing.

Related Topics

System Logs Menu