Alarm setup and definitions in Cisco Unified Serviceability

Set up Cisco Unified IM and Presence Serviceability alarms

Perform the following tasks to set up Cisco Unified IM and Presence Serviceability alarms:

Procedure

Step 1 Select the server and service for which you want the alarm information.

Step 2 Select the destination of the alarm

- All services can go to the SDI (System Diagnostic Interface) log (but must be configured in Trace also).

- All services can go to the SysLog Viewer.

- To send syslog messages to the Remote Syslog Server, check the Remote Syslog destination and specify a host name.

Step 3 Select the alarm event level.

Step 4 If desired, add a definition to an alarm.

Step 5 If you chose an SDI trace file as the alarm destination, collect traces and view the information with the trace and log central option in RTMT.
See the *Cisco Unified Real-Time Monitoring Tool Administration Guide* for more information.

Step 6 If you chose local syslog as the alarm destination, view the alarm information in the SysLog Viewer in RTMT.
See the *Cisco Unified Real-Time Monitoring Tool Administration Guide* for more information.

Step 7   See the corresponding alarm definition for the description and recommended action.

Related Topics

Alarm setup and update for a service

This section provides information to setup and update alarms for a service.

Alarm setup for a service

Cisco Unified IM and Presence Serviceability alarms provide information about runtime status and the state of the system. This information allows you to troubleshoot problems that are associated with your system, for example, to identify issues with the Disaster Recovery System.

You can configure the alarm interface to send alarm information to multiple locations, and each location can have its own alarm event level (from debug to emergency). You can direct alarms to the Syslog Viewer (local syslog), Syslog file (remote syslog), an SDI trace log file, or to all destinations. When a service issues an alarm, the alarm interface sends the alarm information to the locations that you configure (and that are specified in the routing list in the alarm definition) (for example, SDI trace). The system can either forward the alarm information, as is the case with SNMP traps, or the system can write the alarm information to its final destination (such as a log file).

You can configure alarms for services, such as Cisco Database Layer Monitor, on a particular node, or you configure alarms for a particular service on all nodes in the cluster.

To configure an alarm for a service, you select an alarm event level, such as Error, and the location(s), such as Syslog Viewer (local syslog), where you want the system to send the alarm information. Choosing an event level accomplishes the following tasks: helps you narrow the types of alarms that get collected and prevents the Syslog and trace files from becoming overloaded.

You view alarm information to determine whether problems exist. The method that you use to view the alarm information depends on the destination that you chose when you configured the alarm. You can view alarm information that is sent to the SDI trace log file by using the Trace and Log central option in RTMT or by using a text editor. You can view alarm information that is sent to local syslog by using the SysLog Viewer in RTMT.

Set up or update alarm for a service

Perform this procedure to configure or update an alarm for a service. See your online Operating System documentation for more information on how to use your standard registry editor.

Note   Cisco recommends that you do not change SNMP Trap and Catalog configurations.

You can set the alarm destination, see the following table:

Note   The alarm destination options vary depending on the service group and service that you select.

Table 1: Alarm Destinations

Name	Destination description
Enable Alarm for Local Syslogs	SysLog Viewer. The program logs IM and Presence errors in the Application Logs within SysLog Viewer and provides a description of the alarm and a recommended action. You can access the SysLog Viewer from the Serviceability Real-Time Monitoring Tool.
Enable Alarm for Remote Syslogs	Syslog file. Check to enable the Syslog messages to be stored on a Syslog server and to specify the Syslog server name. You can specify up to five Syslog server names. If this destination is enabled and no server name is specified, IM and Presence does not send the Syslog messages. **Note** If you want to send the alarms to Cisco Unified Operations Manager, specify the Cisco Unified Operations Manager server name.
Enable Alarm for SDI Trace	The SDI trace library. Check this to log alarms in the SDI trace log file, and then check Trace On in the Trace Configuration window for the chosen service.

You can also set the event level for the alarm, see the following table:

Table 2: Alarm Event Levels

Name	Description
Emergency	Designates system as unusable.
Alert	Indicates that immediate action is needed.
Critical	IM and Presence detects a critical condition.
Error	Signifies an error condition exists.
Warning	Indicates that a warning condition is detected.
Notice	Designates a normal but significant condition.
Informational	Designates information messages only.

Name	Description
Debug	Designates detailed event information that Cisco TAC engineers use for debugging.

Procedure

Step 1 Select **Alarm** > **Configuration**.

Step 2 Select the server for which you want to configure the alarm from the **Server** list box.

Step 3 Select **Go**.

Step 4 Select the category of service, for example, Database and Admin Services, for which you want to configure the alarm from the **Service Group** list box.

Step 5 Select **Go**.

Step 6 Select the service for which you want to configure the alarm from the **Service** list box.

Step 7 Select **Go**.
  Note   The list box displays all services (active and inactive).

Step 8 Check the required alarm destination.
  The options that display vary depending on the service group and service you select.

Step 9 Select the desired alarm event level from the **Alarm Event Level** list box.

Step 10 Check **Apply to All Nodes** to apply the current settings for selected services to all nodes in a cluster.

Step 11 Perform one of the following actions:
  a) Select **Save** to save your configuration.
  b) Select **Set to Default** to revert to the default settings and select **Save**.

Related Topics

  Set up trace parameters

Alarm definitions and user-defined description additions

This section provides information about alarm definitions and user-defined description additions.

Alarm definitions and user-defined descriptions

Alarm definitions describe alarm messages: what they mean and how to recover from them. You search the **Alarm Definitions** window for alarm information. When you select any service-specific alarm definition, a description of the alarm information (including any user-defined text that you have added) and a recommended action display.

You can search for definitions of all alarms that display in Cisco Unified IM and Presence Serviceability. To aid you with troubleshooting problems, the definitions, which exist in a corresponding catalog, include the alarm name, description, explanation, recommended action, severity, parameters, monitors, and so on.

When the system generates an alarm, it uses the alarm definition name in the alarm information, so you can identify the alarm. In the alarm definition, you can view the routing list, which specifies the locations where the system can send the alarm information. The routing list may include the following locations, which correlate to the locations that you can configure in the **Alarm Configuration** window:

- SDI —The system sends the alarm information to the SDI trace if you enable the alarm for this option and specify an appropriate event level in the **Alarm Configuration** window.

- Sys Log—The system sends the alarm information to the remote syslog server if you enable the alarm for this option, specify an appropriate event level in the **Alarm Configuration** window, and enter a server name or IP address for the remote syslog server.

- Event Log—The system sends the alarm information to the local syslog, which you can view in the SysLog Viewer in the Real-Time Monitoring Tool (RTMT), if you enable the alarm for this option and specify an appropriate event level in the **Alarm Configuration** window.

- Data Collector—System sends the alarm information to the real-time information system (RIS data collector) (for alert purposes only). You cannot configure this option in the **Alarm Configuration** window.

- SNMP Traps—System generates an SNMP trap. You cannot configure this option in the **Alarm Configuration** window.

The system sends an alarm if the configured alarm event level for the specific location in the **Alarm Configuration** window is equal to or lower than the severity that is listed in the alarm definition. For example, if the severity in the alarm definition equals WARNING_ALARM, and, in the **Alarm Configuration** window, you configure the alarm event level for the specific destination as Warning, Notice, Informational, or Debug, which are lower event levels, the system sends the alarm to the corresponding destination. If you configure the alarm event level as Emergency, Alert, Critical, or Error, the system does not send the alarm to the corresponding location.

For each Cisco Unified IM and Presence Serviceability alarm definition, you can include an additional explanation or recommendation. All administrators have access to the added information. You enter information into the User Defined Text pane that displays in the **Alarm Details** window. Standard horizontal and vertical scroll bars support scrolling. Cisco Unified IM and Presence Serviceability adds the information to the database.

View alarm definitions and add user-defined descriptions

Before You Begin

Review the description of alarm definition catalogs.

Procedure

Step 1 Select **Alarm** > **Definitions**.

Step 2 Perform one of the following actions:

a) Select an alarm as follows:

• Select an alarm catalog from the **Find alarms where** list box, for example, a System Alarm catalog or IM and Presence alarm catalog.

• Select the specific catalog name from the **Equals** list box.

b) Enter the alarm name in the **Enter Alarm Name** field.

Step 3 Select **Find**.

Step 4 Perform one of the following actions if multiple pages of alarm definitions exist:

a) To select another page, select the appropriate navigation button at the bottom of the **Alarm Message Definitions** window.

b) To change the number of alarms that display in the window, select a different value from the **Rows per Page** list box.

Step 5 Select the alarm definition for which you want alarm details.

Step 6 Enter text in the **User Defined Text** box if you want to add information to the alarm, and then select **Save**.

Tip If you add text in the **User Defined Text** box, you can select **Clear All** at any time to delete the information that you entered.

Step 7 Select **Save**.

Step 8 Select **Back to Find/List Alarms** from the Related Links list box if you want to return to the **Alarm Message Definitions** window.

Step 9 Select **Go**.

Related Topics

Alarm Catalog descriptions

This section provides alarm catalog descriptions.

System Alarm Catalog descriptions

The following table contains the System Alarm Catalog alarm descriptions.

Table 3: System Alarm Catalogs

Name	Description
ClusterManagerAlarmCatalog	All cluster manager alarm definitions that are related to the establishment of security associations between nodes in a cluster.
DBAlarmCatalog	All Cisco database alarm definitions
DRFAlarmCatalog	All Disaster Recovery System alarm definitions

Name	Description
GenericAlarmCatalog	All generic alarm definitions that all applications share
JavaApplications	All Java Applications alarm definitions. **Tip** You cannot use the alarm configuration GUI to configure JavaApplications alarms. You generally configure these alarms to go to the Event Logs and to generate SNMP traps to integrate with Cisco Unified Operations Manager.
LoginAlarmCatalog	All login-related alarm definitions
LpmTctCatalog	All log partition monitoring and trace collection alarm definitions
RTMTAlarmCatalog	All IM and Presence Real-Time Monitoring Tool alarm definitions
SystemAccessCatalog	All alarm definitions that are used for tracking whether SystemAccess provides all thread statistic counters together with all the process statistic counters.
ServiceManagerAlarmCatalog	All service manager alarm definitions that are related to the activation, deactivation, starting, restarting, and stopping of services.
IMSAlarmCatalog	All user authentication and credential definitions.
CertMonitorAlarmCatalog	All certificate expiration definitions.
EMAlarm	All Extension Mobility alarm definitions
CDPAlarmCatalog	Alarms for Cisco Discovery Protocol (CDP) service.
LBMAlarmCatalog	All Location Bandwidth Manager (LBM) alarm definitions.

IM and Presence Alarm Catalog descriptions

The following table contains the IM and Presence Alarm Catalog description.

Table 4: IM and Presence Alarm Catalog

Name	Description
CiscoUPSConfigAgent	All Config Agent alarms that notify the IM and Presence SIP Proxy of configuration changes in the IM and Presence IDS database.
CiscoUPInterclusterSyncAgent	All Intercluster Sync Agent alarms that enable DND propagation to Cisco Unified Communications Manager and synchronize end user information between IM and Presence clusters for intercluster SIP routing.

Name	Description
CiscoUPSPresenceEngine	All Presence Engine alarms that collect information regarding the availability status and communications capabilities of a user.
CiscoUPSSIPProxy	All SIP Proxy alarms that are related to routing, requestor identification, and transport interconnection.
CiscoUPSSOAP	All SOAP alarms that provide a secure SOAP interface to and from external clients using HTTPS.
CiscoUPSSyncAgent	All Sync Agent alarms that keep IM and Presence data synchronized with Cisco Unified Communications Manager data.
CiscoUPXCP	All XCP alarms that collect information on the status of XCP components and services on IM and Presence.
CiscoUPServerRecoveryManager	All server recovery manager alarms that relate to the failover and fallback process between nodes in a subcluster.
CiscoUPReplWatcher	All ReplWatcher alarms that monitor IDS Replication State.
CiscoUPXCPConfigManager	All Cisco XCP Config Manager alarm definitions that relate to XCP components.

Alarm information, which includes an explanation and recommended action, also includes the application name, server name, and so on, to help you perform troubleshooting, even for problems that are not on your local IM and Presence server.

For more information about the alarms specific to IM and Presence, see the *System Error Messages for IM and Presence on Cisco Unified Communications Manager* at this location: