Trace setup

Set up trace

Perform the following tasks to set up and collect trace for feature and network services in Cisco Unified IM and Presence Serviceability. See the*Cisco Unified Real-Time Monitoring Tool Administration Guide* for more details.

Procedure

Step 1 To enable trace compression, select **Zip Files** under Download File Options during Trace Collection setup.

Step 2 Select **System** > **Service Parameters** in Cisco Unified CM IM and Presence Administration and configure the values of the TLC Throttling CPU Goal and TLC Throttling IOWait Goal service parameters (Cisco RIS Data Collector service).

Step 3 Configure the trace setting for the service for which you want to collect traces. You can configure trace for the service on one server or on all servers in the cluster.
To configure trace settings, select what information you want to include in the trace log by choosing the debug level and trace fields.

If you want to run predetermined traces on services, set troubleshooting trace for those services.

Step 4 Install the Real-Time Monitoring Tool on a local PC.

Step 5 To generate an alarm when the specified search string exists in a monitored trace file, enable the LogFileSearchStringFound alert in RTMT. Do the following:

a) In Cisco Unified IM and Presence Serviceability, select **Alarms** > **Definitions**.
b) In the **Find alarms where** list box, select the **System Alarm Catalog**.
c) in the **Equals** list box, select **LpmTctCatalog**.

Tip You can find the LogFileSearchStringFound alarm in the LpmTctCatalog.

Step 6 To automatically capture traces for alerts such as CriticalServiceDown, check **Enable Trace Download** in the **Set Alert/Properties** dialog box for the specific alert in RTMT; configure how often that you want the download to occur.

Step 7 Collect the traces.

Step 8 View the log file in the appropriate viewer.
See the*Cisco Unified Real-Time Monitoring Tool Administration Guide* for more information.

Step 9 If you enabled troubleshooting trace, reset the trace settings services so the original settings are restored.

Note Leaving Troubleshooting trace enabled for a long time increases the size of the trace files and may impact the performance of the services.

Related Topics

Alarm definitions and user-defined descriptions
Set up trace parameters, on page 6
Troubleshoot trace settings window, on page 16

Trace parameter configuration

Cisco Unified IM and Presence Serviceability provides trace tools to assist you in troubleshooting issues with your Presence and Instant Messaging application. Cisco Unified IM and Presence Serviceability supports:

- SDI (System Diagnostic Interface) trace
- Log4J trace (for Java applications)

You can configure the level of information that you want traced (debug level), what information you want to trace (trace fields), and information about the trace files (such as number of files per service, size of file, and time that the data is stored in the trace files.) You can configure trace for a single service or apply the trace settings for that service to all servers in the cluster.

In the **Alarm Configuration** window, you can direct alarms to various locations, including SDI trace log files. If you want to do so, you can configure trace for alerts in the IM and Presence Real-Time Monitoring Tool (RTMT).

After you have configured information that you want to include in the trace files for the various services, you can collect and view trace files by using the Trace & Log Central option in the RTMT. You can configure trace parameters for any feature or network service that is available on any IM and Presence node in the cluster. Use the **Trace Configuration** window to specify the parameters that you want to trace for troubleshooting problems. If you want to use predetermined troubleshooting trace settings rather than choosing your own trace fields, you can use the **Troubleshooting Trace Setting** window.

Note Enabling Trace decreases system performance; therefore, enable Trace only for troubleshooting purposes. For assistance in using Trace, contact Cisco TAC support.

Related Topics

Set up trace parameters, on page 6

Service groups in trace configuration

The following table lists the services and trace libraries that correspond to the options in the **Service Group** list box in the **Trace Configuration** window.

Table 1: Service Groups in Trace Configuration

Service Group	Services and Trace Libraries	Notes
IM and Presence Services	• Cisco Client Profile Agent • Cisco Config Agent • Cisco Intercluster Sync Agent • Cisco Login Datastore • Cisco OAM Agent • Cisco Presence Datastore • Cisco Presence Engine • Cisco Replication Watcher • Cisco Route Datastore • Cisco SIP Proxy • Cisco SIP Registration Datastore • Cisco Server Recovery Manager • Cisco Sync Agent • Cisco XCP Authentication Service • Cisco XCP Config Manager • Cisco XCP Connection Manager • Cisco XCP Directory Service • Cisco XCP Message Archiver • Cisco XCP Router • Cisco XCP SIP Federation Connection Manager • Cisco XCP Text Conference Manager • Cisco XCP Web Connection Manager • Cisco XCP XMPP Federation Connection Manager	See topics related to feature and network services in Cisco Unified IM and Presence Serviceability for a description of these services. • For these services, you should enable all trace for the service, instead of running trace for specific components. • For the Cisco Sync Agent you can enable trace for specific components.

Service Group	Services and Trace Libraries	Notes
Database and Admin Services	• Cisco AXL Web Service • Cisco Bulk Provisioning Service • Cisco CCMUser Web Service • Cisco Database Layer Monitor • Cisco GRT Communications Web Service • Cisco IM and Presence Admin • Cisco IM and Presence User • Cisco Unified Reporting Web Service • Platform SOAP Services	For most services in the Database and Admin Services group, you enable all trace for the service/library, instead of enabling trace for specific components. For Cisco Database Layer Monitor, you can run trace for specific components. **Note** You can control logging for services in the Cisco Unified IM and Presence Serviceability UI. To change the log level, select the "System Services" group and "Cisco CCMService Web Service" service.
Performance and Monitoring Services	• Cisco AMC Service • Cisco Audit Event Service • Cisco Log Partition Monitoring Tool • Cisco RIS Data Collector • Cisco RTMT Web Service • Cisco RisBean Library	Selecting the Cisco RTMT Web Service option turns on trace for the RTMT servlets; running this trace creates the server-side log for RTMT client queries.
Backup and Restore Services	• Cisco DRF Local • Cisco DRF Master	You enable all trace for each service, instead of running trace for specific components.
System Services	• Cisco CCMService Web Service • Cisco Trace Collection Service	
SOAP Services	• Cisco SOAP Web Service • Cisco SOAPMessage Service	Selecting the Cisco SOAP Web Service option turns on the trace for the AXL Serviceability API. You enable all trace for this service, instead of running trace for specific components.
Platform Services	Cisco Unified OS Admin Web Service	

Related Topics

Feature and network services in Cisco Unified Serviceability

Set up trace parameters

Perform the following procedure to set up the trace parameters. Changes to trace parameter configuration take effect immediately for all services.

Note The Debug Trace Level options that display vary, depending on which service you are tracing.

Use the following table to set the level of information that you want traced.

Table 2: Debug Trace Levels

Level	Description
Arbitrary	Traces all Entry and Exit conditions plus low-level debugging information. **Note** Do not use this trace level with the Cisco IP Voice Media Streaming Application service during normal operation.
Debug	Traces all State Transition conditions plus media layer events that occur during normal operation. **Note** Do not use Debug logging with the Cisco Presence Engine service because this trace level degrades system performance. We strongly recommend that you use the Info trace level to debug issues during normal operation.
Detailed	Traces all Arbitrary conditions plus detailed debugging information. **Note** Do not use Debug logging with the Cisco IP Voice Media Streaming Application service because this trace level degrades system performance. We strongly recommend that you use the Info trace level to debug issues during normal operation.
Entry/Exit	Traces all significant conditions plus entry and exit points of routines. Not all services use this trace level (for example, IM and Presence does not).
Error	Traces alarm conditions and events. Used for all traces that are generated in abnormal path. Uses minimum number of CPU cycles.
Fatal	Traces very severe error events that may cause the application to cancel.
Info	Traces the majority of servlet problems and has a minimal effect on system performance.
Significant	Traces all State Transition conditions plus media layer events that occur during normal operation.

Level	Description
Special	Traces all Error conditions plus process and device initialization messages.
State Transition	Traces all Special conditions plus subsystem state transitions that occur during normal operation.
Warn	Traces potentially harmful situations.

Use the following table to set the trace output limit.

Table 3: Trace Output Limit

Field	Description
Maximum No. of files	This field specifies the total number of trace files for a given service. IM and Presence automatically appends a sequence number to the file name to indicate which file it is; for example, esp000005. When the last file in the sequence is full, the trace data begins writing over the first file. The default varies by service.
Maximum File Size (MB)	This field specifies the maximum size of the trace file in megabytes. The default varies by service.

The following table below describes the service trace filter settings for the IM and Presence SIP Proxy.

Table 4: IM and Presence SIP Proxy Service Trace Filter Settings

Parameter	Description
Enable CTI Gateway Trace	This parameter enables tracing for the CTI Gateway.
Enable Parser Trace	This parameter enables tracing of parser information related to the operation of the per-sipd child SIP parser.
Enable SIP TLS Trace	This parameter enables tracing for information related to the TLS transport of SIP messages by TCP services.
Enable Privacy Trace	This parameter enables tracing for information about processing of PAI, RPID, and Diversion headers in relation to privacy requests.
Enable Routing Trace	This parameter enables tracing for the Routing module.
Enable SIPUA Trace	This parameter enables tracing for the SIP UA application module.
Enable Number Expansion Trace	This parameter enables tracing for the Number Expansion module.

Parameter	Description
Enable Presence Web Service Trace	This parameter enables tracing for the Presence Web Service.
Enable SIP Message and State Machine Trace	This parameter enables tracing for information related to the operation of the per-sipd SIP state machine.
Enable SIP TCP Trace	This parameter enables tracing for information related to the TCP transport of SIP messages by TCP services.
Enable Authentication Trace	This parameter enables tracing for the Authentication module.
Enable Enum Trace	This parameter enables tracing for the Enum module.
Enable Registry Trace	This parameter enables tracing for the Registry module.
Enable Method/Event Routing Trace	This parameter enables tracing for the Method/Event routing module.
Enable CALENDAR Trace	This parameter enables tracing for the Calendar module.
Enable Server Trace	This parameter enables tracing for the Server.
Enable Access Log Trace	This parameter enables the proxy access log trace; the first line of each SIP message received by the proxy is logged.
Enable SIP XMPP IM Gateway Trace	This parameter enables trace for the SIP XMPP IM Gateway.

Before You Begin

Review the tasks in the trace set up and collection procedure.

Procedure

Step 1 Select **Trace** > **Configuration**.

Step 2 Perform the following actions:

a) Select the server that is running the service for which you want to configure trace from the **Server** list box.

b) Select **Go**.

c) Select the service group for the service that you want to configure trace from the Service Group list box. Table 1: Service Groups in Trace Configuration, on page 4 lists the services and trace libraries that correspond to the options that display in the **Service Group** list box, and then select **Go**.

d) Select the service for which you want to configure trace from the **Service** list box, and then select **Go**. The list box displays all services (active and inactive).

Note Depending on the service you select and the traces generated by that service, some trace fields may be disabled or selected by default on the **Trace Configuration** screen.

Note The section in the **Trace Filter Settings** area that relates to devices is not relevant to IM and Presence.

Step 3 If you configured Troubleshooting Trace for this service, a message displays at the top of the window that indicates that Troubleshooting Traces have been set. The system disables all fields on the window except the Output Settings. To configure the Output Settings, go to step 9.

Step 4 Check **Apply to All Nodes** if you want trace to apply to all IM and Presence servers in the cluster.

Step 5 Check **Trace On** .

Step 6 Select the level of information that you want traced from the **Debug Trace Level** list box.

Step 7 Check the relevant trace check boxes for the service that you chose; for example, Cisco SIP Proxy Trace Fields check box.

Step 8 Check the trace fields that you want to enable if the service that you chose has multiple trace fields, such as the Cisco SIP Proxy service.

Step 9 Specify the trace output setting to limit the number and size of the trace files.

Note When you change either the Maximum number of files or Maximum file size (MB) parameter, the system deletes all the service log files except the current file if the service is running, or, if the service is not active, the system will delete the files when the service is initially turning on. If you want to keep a record of the log files, make sure that you download and save the service log files to another server before changing the **Maximum No. of Files** parameter or the **Maximum File Size** parameter.

Step 10 Perform one of the following actions:

a) Select **Save** to save your trace parameters configuration.

b) Select **Set Default** to set the default.

Related Topics

Set up trace, on page 1
Service groups in trace configuration, on page 3
Trace field descriptions
Troubleshoot trace settings window, on page 16

Audit log configuration

With audit logging, specific changes to the IM and Presence service get logged in separate log files for auditing: system audit logs, application audit logs, and database audit logs.

System audit logs

System audit logs track activities such as the creation, modification, or deletion of Linux OS users, log tampering, and any changes to file or directory permissions. This type of audit log is disabled by default due to the high volume of data gathered. To enable this function, you must manually enable utils auditd using the CLI. After you have enabled the system audit log feature, you can collect, view, download, or delete selected logs through Trace & Log Central from the Real-Time Monitoring Tool. System audit logs take on the format of `vos-audit.log`.

For information about how to enable this feature, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*. For information about how to access collected logs from the Real-Time Monitoring Tool, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide* .

Application audit logs

The Application Audit logs track configuration changes to the IM and Presence service and are stored in separate log files for auditing purposes. The Cisco Audit Event Service, which appears under Control Center—Network Services in Cisco Unified IM and Presence Serviceability, writes the Application Audit logs. The Application Audit logs monitor and record any configuration change to the IM and Presence service by a user or as a result of the user action.

You access the **Audit Log Configuration** window in Cisco Unified IM and Presence Serviceability to configure the settings for these audit logs.
Audit logging contains the following parts:

- Audit logging framework—The framework comprises an API that uses an alarm library to write audit events into audit logs. An alarm catalog that is defined as GenericAlarmCatalog.xml applies for these alarms. Different IM and Presence components provide their own logging.

  The following example displays an API that an IM and Presence component can use to send an alarm:

  ```
  User ID: CUPAdministrator

  Client IP Address: 172.19.240.207

  Severity: 3

  EventType: ServiceStatusUpdated

  ResourceAccessed: CUPService

  EventStatus: Successful

  Description: CiscoUnifiedPresence Service status is stopped
  ```

- Audit event logging—An audit event represents any event that is required to be logged. The following example displays a sample audit event:

  ```
  CUP_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated

  UserID:CUPAdministrator Client IP Address:172.19.240.207 Severity:3

  EventType:ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:

  Successful Description: Cisco Unified Presence Service status is stopped App ID:Cisco

  Tomcat Cluster ID:StandAloneCluster Node ID:sa-cm1-3
  ```

Tip Be aware that audit event logging is centralized and enabled by default. An alarm monitor called Syslog Audit writes the logs. By default, the logs are configured to rotate. If the AuditLogAlarmMonitor cannot write an audit event, the AuditLogAlarmMonitor logs this failure as a critical error in the syslog file. The Alert Manager reports this error as part of a SeverityMatchFound alert. The actual operation continues even if the event logging fails. All audit logs get collected, viewed and deleted from Trace and Log Central in the IM and Presence Real-Time Monitoring Tool.

The following components generate audit events:

- IM and Presence Application
- Cisco Unified IM and Presence Serviceability
- Cisco Unified IM and Presence Real-Time Monitoring Tool
- Cisco Unified CM IM and Presence Administration
- Command Line Interface

Cisco Unified IM and Presence Serviceability

Cisco Unified IM and Presence Serviceability logs the following events:

- Activation, deactivation, start, or stop of a service
- Changes in trace configurations and alarm configurations
- Changes in SNMP configurations
- Review of any report in the Serviceability Reports Archive. This log gets viewed on the reporter node

Cisco Unified IM and Presence Real-Time Monitoring Tool

Cisco Unified IM and Presence Real-Time Monitoring Tool logs the following events with an audit event alarm:

- Alert configuration
- Alert suspension
- E-mail configuration
- Set node alert status
- Alert addition
- Add alert action
- Clear alert
- Enable alert
- Remove alert action
- Remove alert

Cisco Unified CM IM and Presence Administration

The following events get logged for various components of Cisco Unified CM IM and Presence Administration:

- Administrator logging (logins and logouts on IM and Presence interfaces such as Administration, OS Administration, Disaster Recovery System, and Reporting)
- User role membership updates (user added, user deleted, user role updated)
- Role updates (new roles added, deleted, or updated)
- Device updates (phones and gateways)

- Server configuration updates (changes to alarm or trace configurations, service parameters, enterprise parameters, IP addresses, host names, Ethernet settings, and IM and Presence server additions or deletions)

IM and Presence Application

The following events get logged by the various components of the IM and Presence Application:

- End user logging on IM clients (user logins, user logouts, and failed login attempts)
- User entry to and exit from IM Chat Rooms
- Creation and destruction of IM Chat Rooms

Command Line Interface

All commands issued via the command line interface are logged.

Database audit logs

Database Audit Logs track all activities associated with access to the Informix Database, such as logins.

Configure audit log settings

To configure Application Audit Log or Database Audit Log settings, perform the following procedure:

Note The Application Audit Logs (Linux auditd) can only be enabled or disabled through the CLI. Other than the collection of vos-audit.log through the Real-Time Monitoring Tool, you can not change any settings for this type of audit log.

Procedure

Step 1 In Cisco Unified IM and Presence Serviceability, select **Tools** > **Audit Log Configuration**.
The **Audit Log Configuration** window displays.

Step 2 Configure the settings as described in Audit log settings, on page 12.

Step 3 Select **Save**.

Audit log settings

The following table describes the settings that you can configure in the **Audit Log Configuration** window in Cisco Unified IM and Presence Serviceability. Settings can be configured for Application Audit Logs and Database Audit Logs.

Before you begin

Be aware that only a user with an audit role can change the audit log settings. By default, for IM and Presence, the administrator possesses the audit role after fresh installs and upgrades. The administrator can assign any user that has auditing privileges to the Standard Audit Users group in the **User Group Configuration** window. If you want to do so, you can then remove administrator from the Standard Audit Users group.

The Standard Audit Log Configuration role in IM and Presence provides the ability to delete audit logs and to read/update access to IM and Presence Real-Time Monitoring Tool, Trace Collection Tool, RTMT Alert Configuration, Control Center—Network Services in Cisco Unified IM and Presence Serviceability, RTMT Profile Saving, Audit Configuration in Cisco Unified IM and Presence Serviceability, and a resource that is called Audit Traces.

For information on roles, users, and user groups in IM and Presence, refer to the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Table 5: Audit Log Configuration Settings

Field	Description
Select Server	
Server	Select the server where you want to configure audit logs; then, select **Go.**
Apply to All Nodes	If you want to apply the audit log configuration to all nodes in the cluster, check the **Apply to All Nodes** box.
Application Audit Log Settings	
Enable Audit Log	This setting configures the Application Audit logs. When you enable this setting, an audit log gets created for the Application Audit log. For IM and Presence, the application audit log supports configuration updates for IM and Presence graphical user interfaces (GUIs), such as Cisco Unified CM IM and Presence Administration, Cisco Unified IM and Presence Real-Time Monitoring Tool, and Cisco Unified IM and Presence Serviceability. **Note** The Network Service Audit Event Service must be running.
Enable Text Conferencing Audit Log	

Enable Purging	The Log Partition Monitor (LPM) looks at the Enable Purging option to determine whether it needs to purge audit logs. When you check this check box, LPM purges all the audit log files in RTMT whenever the common partition disk usage goes above the high water mark; however, you can disable purging by unchecking the check box. If purging is disabled, the number of audit logs continues to increase until the disk is full. This action could cause a disruption of the system. A message that describes the risk of disabling the purge displays when you uncheck the **Enable Purging** check box. Be aware that this option is available for audit logs in an active partition. If the audit logs reside in an inactive partition, the audit logs get purged when the disk usage goes above the high water mark. You can access the audit logs by selecting **Trace and Log Central** > **Audit Logs** in RTMT. **Note** The Network Service Cisco Log Partitions Monitoring tool must be running.
Enable Log Rotation	The system reads this option to determine whether it needs to rotate the audit log files or it needs to continue to create new files. The maximum number of files cannot exceed 5000. When the Enable Rotation option is checked, the system begins to overwrite the oldest audit log files after the maximum number of files gets reached. **Tip** When log rotation is disabled (unchecked), audit log ignores the **Maximum No. of Files** setting.
Server Name	Enter the name or IP address of the remote Syslog server that you want to use to accept Syslog messages. If server name is not specified, Cisco Unified IM and Presence Serviceability does not send the Syslog messages. Do not specify a Cisco Unified Communications Manager server as the destination because the Cisco Unified Communications Manager server does not accept Syslog messages from another server.
Remote Syslog Audit Event Level	Select the desired Syslog messages severity for the remote syslog server. All the syslog messages with selected or higher severity level are sent to the remote syslog.
Maximum No. of Files	Enter the maximum number of files that you want to include in the log. The default setting specifies 250. The maximum number specifies 5000.

Maximum File Size	Enter the maximum file size for the audit log. The file size value must remain between 1 MB and 10 MB.
Database Audit Log Filter Settings	
Enable Audit Log	When you enable this check box, DB audit log gets created for the IM and Presence database. Use this setting in conjunction with the **Debug Audit Level** setting, which allows you create a log for certain aspects of the database.
Debug Audit Level	This setting allows you to choose which aspects of the database you want to audit in the log. From the drop-down list box, select one of the following options. Be aware that each audit log filter level is cumulative. • **Schema**—Tracks changes to the setup of the audit log database (for example, the columns and rows in the database tables). • **Administrative Tasks**—Tracks all administrative changes to the IM and Presence system (for example, any changes to maintain the system) plus all Schema changes. **Tip** Most administrators will leave the **Administrative Tasks** setting disabled. For users who want auditing, use the Database Updates level. • **Database Updates**—Tracks all changes to the database plus all schema changes and all administrative tasks changes. • **Database Reads**—Tracks every read to the IM and Presence system, plus all schema changes, administrative tasks changes, and database updates changes. **Tip** Select the Database Reads level only when you want to get a quick look at the IM and Presence system. This level uses significant amounts of system resources and only should be used for a short time.

Enable Audit Log Rotation	The system reads this option to determine whether it needs to rotate the database audit log files or it needs to continue to create new files. When the **Enable Audit Log Rotation** option is checked, the system begins to overwrite the oldest audit log files after the maximum number of files gets reached. When this setting is unchecked, audit log ignores the **Maximum No. of Files** setting.
Maximum No. of Files	Enter the maximum number of files that you want to include in the log. Ensure that the value that you enter for the **Maximum No. of Files** setting is greater than the value that you enter for the **No. of Files Deleted on Log Rotation** setting. You can enter a number from 4 (minimum) to 40 (maximum).
No. of Files Deleted on Log Rotation	Enter the maximum number of files that the system can delete when database audit log rotation occurs. The minimum that you can enter in this field is 1. The maximum value is 2 numbers less than the value that you enter for the **Max No. of Files** setting; for example, if you enter 40 in the **Max No. of Files** field, the highest number that you can enter in the **No. of Files Deleted on Log Rotation** field is 38.

Trace setting troubleshooting

Troubleshoot trace settings window

The **Troubleshooting Trace Settings** window allows you to select the services in Cisco Unified IM and Presence Serviceability for which you want to set predetermined troubleshooting trace settings. In this window, you can select the services on different IM and Presence nodes in the cluster. This populates the trace settings changes for all the services you choose. You can select specific active services for a single node, all active services for the node, specific active services for all nodes in the cluster, or all active services for all nodes in the cluster. In the window, N/A displays next to inactive services.

Note The predetermined troubleshooting trace settings for an IM and Presence feature or network service include SDI, and Log4j trace settings. Before the troubleshooting trace settings are applied, the system backs up the original trace settings. When you reset the troubleshooting trace settings, the original trace settings get restored.

When you open the **Troubleshooting Trace Settings** window after you apply troubleshooting trace settings to a service, the service that you set for troubleshooting displays as checked. In the **Troubleshooting Trace Settings** window, you can reset the trace settings to the original settings.

After you apply Troubleshooting Trace Setting to a service, the **Trace Configuration** window displays a message that troubleshooting trace is set for the given service(s). From the **Related Links** list box, you can select the Troubleshooting Trace Settings option if you want to reset the settings for the service. For the given service, the **Trace Configuration** window displays all the settings as read-only, except for some parameters of trace output settings; for example, Maximum No. of Files.

Troubleshoot trace settings

Before You Begin

Review the tasks in the trace configuration and collection procedure.

Procedure

Step 1 Select **Trace** > **Troubleshooting Trace Settings**.

Step 2 Select the server where you want to troubleshoot trace settings from the **Server** list box.

Step 3 Select **Go**.
A list of services display. The services that are not active on an IM and Presence node display as N/A.

Step 4 Perform one of the following actions:

a) To monitor specific services on the node that you selected from the **Server** list box, check the service in the **Services** pane.
For example, the Database and Admin Services, Performance and Monitoring Services, or the Backup and Restore Services pane (and so on).

This task affects only the node that you selected from the **Server** list box.

b) To monitor all services on the node that you selected from the **Server** list box, check **Check All Services**.

c) To monitor specific services on all nodes in a cluster, check **Check Selected Services on All Nodes**.
This setting applies for all nodes in the cluster where the service is active.

d) To monitor all services for all nodes in the cluster, check **Check All Services on All Nodes**.

Step 5 Select **Save**.

Step 6 Select one of the following buttons to restore the original trace settings:

a) **Reset Troubleshooting Traces**—Restores the original trace settings for the services on the node that you chose in the Server list box; also displays as an icon that you can select.

b) **Reset Troubleshooting Traces On All Nodes**—Restores the original trace settings for the services on all nodes in the cluster.
The Reset Troubleshooting Traces button displays only if you have set troubleshooting trace for one or more services.

Note Leaving Troubleshooting trace enabled for a long time increases the size of the trace files and may impact the performance of the services.

After you select the **Reset** button, the window refreshes and the service check boxes display as unchecked.

Related Topics

Set up trace, on page 1