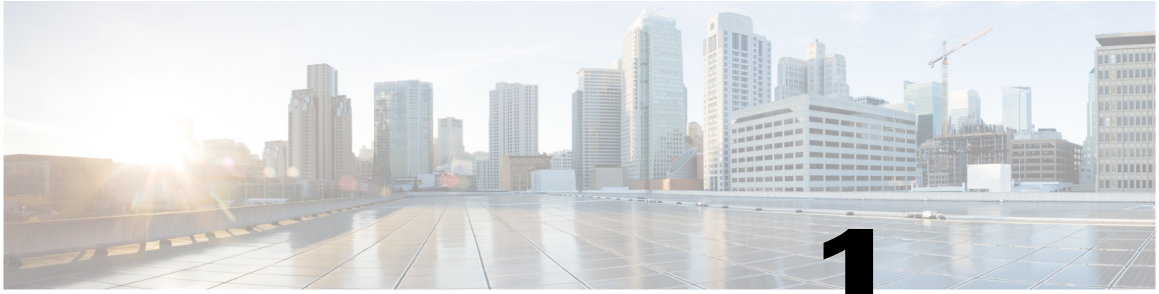
Instant Messaging Compliance for IM and Presence Service on Cisco Unified Communications Manager, Release 11.5(1)

First Published: June 08, 2016

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Planning for IM Compliance

About IM Compliance

Many industries require that instant messages adhere to the same regulatory compliance guidelines as for all other business records. To comply with these regulations, your system must log and archive all business records, and the archived records must be retrievable.

The Cisco Unified Communications Manager IM and Presence Service provides support for instant messaging (IM) compliance by collecting data for the following IM activities in single cluster, intercluster, or federated network configurations:

- Point-to-point messages.
- Group chat - This includes ad-hoc, or temporary chat messages, and permanent chat messages.

IM Compliance Components

IM compliance includes these components:

- IM and Presence Service Release 10.0.(1). IM and Presence Service uses the Message Archiver component for logging messages to the external database.
- External database—For information on supported external databases, see the *Database Setup Guide for IM and Presence Service*.
- IM Client—Supported clients include Cisco clients such as Cisco Jabber; third-party XMPP clients, and other third-party clients used in federated networks.

Note The Message Archiver provides a basic IM logging solution. If you require a more granular logging solution, for example logging based on policy, use the third-party compliance solution, see the appendix module for details.

Related Topics

Database Setup for IM and Presence Service on Cisco Unified Communications Manager, Release 9.0(1)

Integration with Third-Party Compliance Servers, on page 15

Sample Topologies and Message Flow for IM Compliance

Note The external database requirements defined in this section depend on the capacity of your servers.

IM compliance provides logging of all compliance related data to an external database. All IM traffic passes through the IM and Presence Service node (via the message archiver component) and is simultaneously logged to the external database. Each IM log contains the sender and recipient information, the timestamp, and the message body.

For ad hoc group chat messages, by default IM and Presence Service logs multiple copies of the same message to the external database, one copy for each recipient. This identifies what users in the ad hoc group chat received the message.

Depending on the XMPP client you deploy, you may also notice this behavior:

- IM and Presence Service may log an incoming message to the external database twice. This occurs because some XMPP clients do not support the ability to learn the full JID, or address, of the other party in the conversation. Consequently the XMPP client forks the message to *all* active clients for the user (all clients that the user is currently signed into), and IM and Presence Service then logs all forked messages to the external database.
- IM and Presence Service may log the first message in a chat to the external database twice. This occurs until the XMPP client learns the full JID, or address, of the other party in the conversation.

If the IM and Presence Service loses its connection to the external database, it continues to send and deliver IMs to users, and users can still create (ad hoc) chat rooms. However, with no connection to the external database, the IM and Presence Service does not log any of these IMs. To maintain group chat support in this case, persistent chat should be assigned to a different database server. IM and Presence Service raises an alarm if the connection to the external database is lost.

Single Cluster Configuration

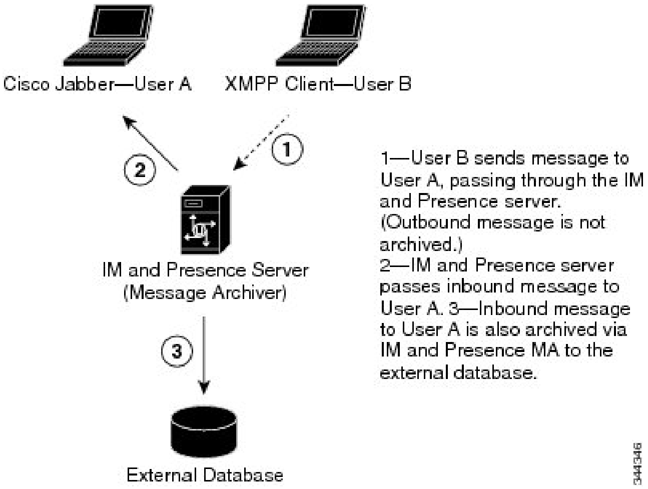
When using IM compliance in a single cluster, we highly recommend that you deploy one external database per cluster to which all incoming messages sent to users in the cluster are logged.

Note

- For IM compliance, we highly recommend that you deploy one external database per cluster. However, depending on your requirements, you can configure more than one external database per cluster, or share an external database between clusters.
- If you deploy the group chat feature, you *require* one external database *per node* in a cluster. See *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* .

The image below highlights these components and message flow. By default IM compliance logs inbound messages to the external database, however you can configure the feature to also log outgoing messages.

Figure 1: IM Compliance for a Single Cluster

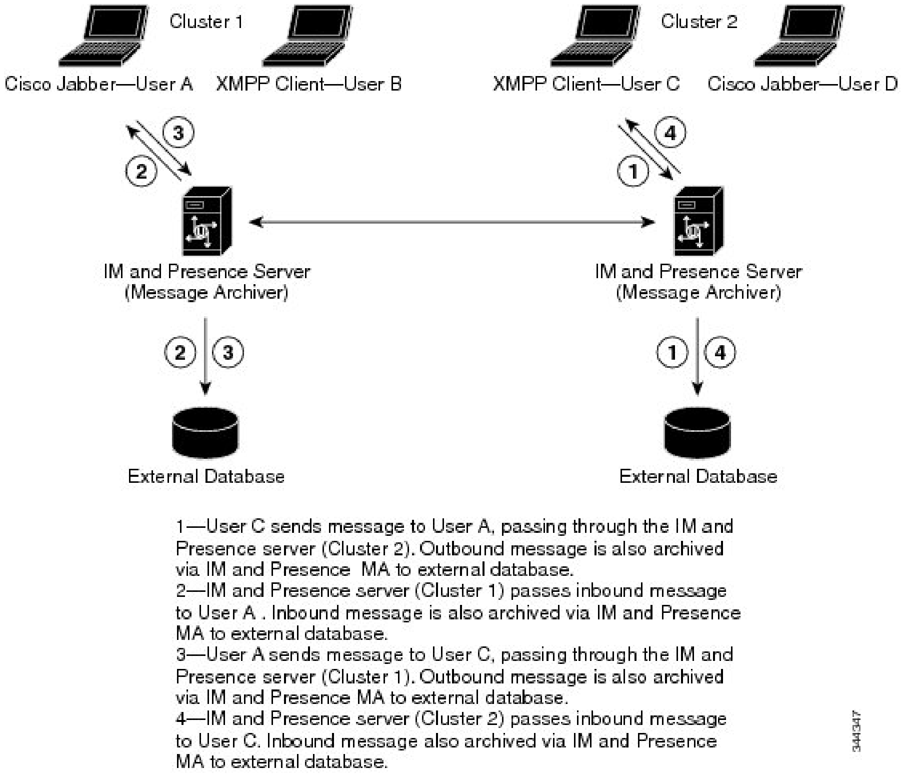

Cisco Jabber—User A
XMPP Client—User B
2
1
IM and Presence Server
(Message Archiver)
3
External Database
1—User B sends message to User A, passing through the IM and Presence server. (Outbound message is not archived.)
2—IM and Presence server passes inbound message to User A. 3—Inbound message to User A is also archived via IM and Presence MA to the external database.
344346

Intercluster or Federated Network Configuration

When using IM compliance in an intercluster or federated network configuration, you must configure an external database per cluster. Additionally, you should configure the IM and Presence Service node to log both incoming and outgoing messages. Otherwise, each database will retain only half of the conversation.

The figure below highlights these components and message flow.

Figure 2: IM Compliance for Multiple Clusters



1—User C sends message to User A, passing through the IM and Presence server (Cluster 2). Outbound message is also archived via IM and Presence MA to external database.
2—IM and Presence server (Cluster 1) passes inbound message to User A . Inbound message is also archived via IM and Presence MA to external database.
3—User A sends message to User C, passing through the IM and Presence server (Cluster 1). Outbound message is also archived via IM and Presence MA to external database.
4—IM and Presence server (Cluster 2) passes inbound message to User C. Inbound message also archived via IM and Presence MA to external database.

Prerequisite Configuration Tasks

Before you use this guide to configure IM compliance, make sure that you have performed the following tasks:

- Install the IM and Presence Service nodes as described in *Installing Cisco Unified Communications Manager*.
- Configure the IM and Presence Service nodes as described in *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.
- Set up the external database as described in *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* .

Support for PostgreSQL 10.0.1

To deploy PostgreSQL version 10.0.1 as the external database, you must set the following values in the postgresql.conf file:

- `escape_string_warning = off`
- `standard_conforming_strings = off`

After you configure these parameters, you must restart PostgreSQL. For more information about how to configure the postgresql.conf file and restart PostgreSQL, see *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* .

Support for Oracle

- In compliance with XMPP specifications, the IM and Presence Service node uses UTF8 character encoding. This allows the node to operate using many languages simultaneously and to display special language characters correctly in the client interface. If you want to use Oracle with the node, you must configure it to support UTF8.
- The value of the **NLS_LENGTH_SEMANTIC** parameter should be set to **BYTE**.
- To determine the tablespace available for your Oracle database, execute the following query as sysdba:

  SELECT DEFAULT_TABLESPACE FROM DBA_USERS WHERE USERNAME = 'UPPER_CASE_USERNAME';

CHAPTER 2

IM Compliance Configuration

Configure IM Compliance

We recommend that you perform this configuration on the publisher node in your cluster.

Before You Begin

- Install and configure one or more supported external databases. Refer to the *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* .
- Configure the external databases on IM and Presence Service. Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **External Databases**.
- Make sure that the trace level for the Cisco XCP Router service is set to info or higher.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Compliance** > **Compliance Settings**.

Step 2 Choose Message Archiver from the Compliance Server Selection.

Step 3 (Optional) Check the **Enable Outbound Message Logging** checkbox.
Turning on this option can degrade IM performance. Because all inbound messages are already logged, do not enable this setting unless you are using IM compliance in intercluster or federated networks.

Step 4 For each node, assign a database from the External Database option.
If you are using one external database for your cluster, assign all nodes to the same external database. If you are using more than one external database for your cluster, assign the nodes to the external databases based on your capacity requirements.

Step 5 Click **Save**.

Step 6 Start the Cisco Message Archiver service (if this service is not already started).

Step 7 Restart the Cisco XCP Router service.
Troubleshooting Tips

a) If you make any subsequent changes to the Message Archiver configuration, restart the Cisco XCP Router service.
b) (All releases) If you switch between IM compliance deployment options (for example, switch from the Third-Party Compliance Server option to the Message Archiver option), you must restart the Cisco XCP Router service.

What to Do Next

Turning on Cisco XCP Message Archiver Service, on page 8

Related Topics

Set Trace Level to Info to Support IM Compliance, on page 12
Restart Cisco XCP Router Service, on page 11
Restart Cisco XCP Message Archiver Service, on page 12
Sample Topologies and Message Flow for IM Compliance, on page 2

Turning on Cisco XCP Message Archiver Service

The Cisco XCP Message Archiver service must be running for the compliance feature to operate correctly on IM and Presence Service.

Note If you do not assign an external database to a node for the compliance feature, IM and Presence Service does not permit you to turn on the Cisco XCP Message Archiver service.

Procedure

Step 1 Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Service Activation**.

Step 2 Choose the server from the Server list box.

Step 3 Click Go.

Step 4 Click the radio button next to the Cisco XCP Message Archiver service in the IM and Presence Services section.

Step 5 Click Save.
Troubleshooting Tips

If the Cisco XCP Message Archiver service fails to start, but the System Troubleshooter (**Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**) shows that the status of the external database connection is ok, we recommend that you unassign the external database from the node, and reassign it again.

Related Topics

Configure IM Compliance, on page 7

CHAPTER 3

IM Compliance Serviceability and Troubleshooting

Restart Cisco XCP Router Service

Procedure

Step 1 Choose**Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Network Services**.

Step 2 Choose the server from the Server list box.

Step 3 Click **Go**.

Step 4 Click the **Cisco XCP Router** radio button in the IM and Presence Services section.

Step 5 Click **Restart**.

Step 6 Click **OK** when a message indicates that restarting may take a while.

Restart Cisco XCP Message Archiver Service

Procedure

Step 1 Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services**.

Step 2 Choose the server from the Server list box.

Step 3 Click **Go**.

Step 4 Click the **Cisco XCP Message Archiver** radio button in the IM and Presence Services section.

Step 5 Click **Restart**.

Set Trace Level to Info to Support IM Compliance

The Message Archiver component uses the logging feature of the Cisco XCP Router service which requires that the trace level is set to Info or higher.

Note IM and Presence Service sets the trace level for Cisco XCP Router to Info by default. If you change the trace level to a level below Info, the compliance feature will not function correctly on IM and Presence Service.

Procedure

Step 1 Sign in to Cisco Unified CM IM and Presence Administration.

Step 2 Choose**Navigation** > **Cisco Unified IM and Presence Serviceability** from the menu in the upper, right corner of the IM and Presence Service main window.

Step 3 Choose**Trace** > **Configuration**.

Step 4 Choose the server that is running the service for which you want to configure trace from the Server list box and click **Go**.

Step 5 Choose IM and Presence Services from the Service Group list box and click **Go**.

Step 6 Choose the Cisco XCP Router service from the Service list box and click **Go**.

Step 7 Check the **Trace On** check box.

Step 8 Choose Info as the Debug Trace Level in the **Trace Filter Settings**.

Configure Alarms for IM Compliance

If IM and Presence Service loses its connection to the external database, users will still be able to send instant messages to each other. However, these messages will not be archived, and you will no longer be satisfying any regulatory compliance guidelines. To ensure that you are notified if this connection is lost, you should verify that its associated alarm is properly configured.

Procedure

Step 1 Sign into **Cisco Unified CM IM and Presence Administration**.

Step 2 Choose **Navigation** > **Cisco Unified IM and Presence Serviceability** from the menu in the upper, right corner of the IM and Presence Service main window.

Step 3 Choose **Alarm** > **Configuration**.

Step 4 From the Server drop-down list, choose the server for which you want to configure the alarm.

Step 5 Click **Go**.

Step 6 From the Service Group drop-down list, choose IM and Presence Services.

Step 7 Click **Go**.

Step 8 From the Service drop-down list, choose Cisco XCP Message Archiver.

Step 9 Click **Go**.

Step 10 Configure the alarm settings as preferred.

Step 11 Click **Save**.

CHAPTER 4

Integration with Third-Party Compliance Servers

About Third-Party Compliance

With this solution, IM and Presence Service integrates with one or more third-party compliance servers for compliance logging or ethical wall functionality. The IM and Presence Service administrator can select which IM, presence, or group chat events are passed to the compliance server(s), and which events are blocked. The events must be selected based on policy. For example, the system could be configured to filter IMs between certain users, or groups of users, and block or modify content depending on the originator and recipient of the IMs.

To use the third-party compliance solution you must configure the third-party compliance server(s) for your cluster. IM and Presence Service passes all configured events that are generated in the processing of user login, logout, presence sharing, IM exchange, or group chat activity to the third-party server(s). The third-party compliance server applies any relevant policy or filtering to the event, then instructs IM and Presence Service as to whether the event should be processed further. Note that you may potentially experience performance delays in your network because of the volume of events that pass between IM and Presence Service and the third-party compliance server. If IM and Presence Service loses its connection to the third-party server, all IM traffic stops.

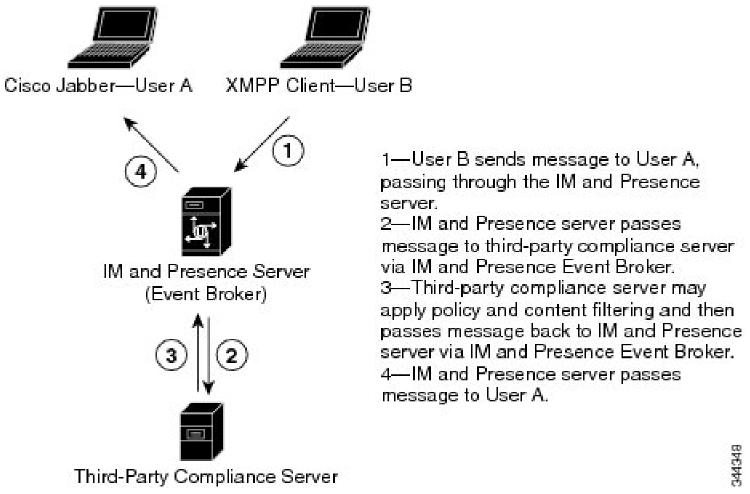
Third-party compliance requires these components:

- IM and Presence Service Release 10.0(x) - IM and Presence Service uses the Event Broker component to send events to the third-party compliance server.
- Third-party compliance server - All IM and Presence Service nodes in the cluster will redirect events to the configured compliance server(s) unless you are upgrading from a system with compliance already configured.
- IM Client - Supported clients include Cisco clients such as Cisco Jabber, third-party XMPP clients, and other third-party clients used in federated networks.

Note IM and Presence Service does not provide a secure TLS/SSL connection between IM and Presence Service and the third-party compliance server.

The following figure highlights the third-party compliance components and message flow.

Figure 3: Third-Party Compliance



1—User B sends message to User A, passing through the IM and Presence server.
2—IM and Presence server passes message to third-party compliance server via IM and Presence Event Broker.
3—Third-party compliance server may apply policy and content filtering and then passes message back to IM and Presence server via IM and Presence Event Broker.
4—IM and Presence server passes message to User A.

Third-Party Compliance Server Configuration Workflow

If you are configuring a third-party compliance integration for the first time, the following workflow is suggested:

Procedure

Step 1 Install third-party compliance servers according to respective compliance vendor documentation.

Step 2 Configure third-party compliance servers on IM and Presence Service nodes. See Configure third-party compliance server on IM and Presence Service below.

Step 3 Configure compliance profiles, selecting events according to respective compliance vendor requirements. See also Compliance profiles below.

Step 4 Configure Compliance Profile Routing Priority if applicable. See Compliance profiles routing priority below.

Step 5 Assign compliance servers and compliance profiles to IM and Presence Service nodes. See Assigning compliance profiles to compliance servers and Assign third-party compliance server to IM and Presence Service node below.

Step 6 On the compliance servers, configure the corresponding open-port names generated by IM and Presence Service according to respective compliance vendor documentation.

Configure Third-Party Compliance Server on IM and Presence Service

Before You Begin

- Install and configure the third-party compliance server(s)
- Install the IM and Presence Service nodes as described in *Installing Cisco Unified Communications Manager*.
- Configure the IM and Presence Service nodes as described in *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

Note Use caution when changing these settings. If you save any changes, you lose all previous configuration settings.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **External Server Setup** > **Third-Party Compliance Servers**.

Step 2 Click Add New.

Step 3 Enter the compliance server name, optional description, Hostname/IP address, port, and password.
The name is only used locally by IM and Presence Service. The IP address, port, and password must match the configuration on the compliance server itself.

Note For the Hostname/IP Address field, allowed characters are all alphanumeric characters (a-zA-Z0-9), period (.), backslash (\), dash (-), and underscore (_).

Step 4 Click Save.

Caution Changes to IP address, port, or password may require corresponding changes on the compliance server for the feature to continue working.

Compliance Profiles

A compliance profile contains a set of Jabber Session Manager (JSM) and\or Text Conferencing (TC) events that you can use to monitor for compliance. You can create a compliance profile that consists of only JSM events, only TC events, or a combination of both JSM and TC events.

When you configure a compliance profile, choose which JSM and TC events you wish to be logged to the compliance server. You can also decide what type of handling is performed by the compliance server, how IM and Presence Service handles error responses from the compliance server, and whether the IM and Presence Service node waits for a response from the compliance server before processing the event further. You can also configure how the events should be processed if no response is expected.

The following tables describe the JSM events and parameters.

Caution If a combination of Bounce, and Fire and Forget is selected, an event to which this applies will be passed to the compliance server and then discarded. This means it will not be processed further by IM and Presence Service. Use this combination with care.

Table 1: JSM Events

Event	Description
e_SESSION	Packets sent during login, which is the creation of a new session.
e_OFFLINE	Packets sent to users who are offline. Offline users are users who do not have an active session.
e_SERVER	Packets sent directly to the server for internal handling.
e_DELIVER	The first event for packets coming in from another server; the second event for packets coming in from a user on the same server. (The first event for packets coming in from the same server is es_IN.)
e_AUTH	IQ packets sent during authentication.
e_REGISTER	Packets generated during registration of a new account by a user.
e_STATS	Packets sent periodically that contain server statistics.
e_DISCOFEAT	Triggered when a user sends a disco#info query.

Event	Description
e_PRISESSION	Determines a user's primary or default session when the user has more than one session. An EventBroker component may dictate the choice of a user's primary session.
es_IN	Generated when a stanza is about to be received by a user's session.
es_OUT	Generated when a stanza is sent from a user's session.
es_END	Packets generated when a user logs out.

Table 2: JSM Parameters

Parameter	Description
Packet Type	Select one of the following XMPP packet types: • **all** - All packets • **iq** - Packets used during info-query functions • **message** - Packets containing standard IM or group chat messages • **presence** - Packets containing presence information • **subscription -** Packets sent when subscribing to another user's presence
Handling	Select **bounce** if errors returned from the compliance server should be bounced back to the originating party or component Select **pass** if they should be discarded.
Fire and Forget	Leave the check box unchecked if the IM and Presence Service node must wait for a response from the compliance server before it continues to process the event. Check the check box if the IM and Presence Service node does not require a response from the compliance server before it continues to process the event further.

The following tables describe the TC events and parameters.

⚠ **Caution** If a combination of Bounce, and Fire and Forget is selected, an event to which this applies will be passed to the compliance server and then discarded. This means it will not be processed further by IM and Presence Service. Use this combination with care.

Table 3: TC Events

Event	Description
onServicePacket	The system receives a packet from the router that is either addressed directly to the TC service or to a room that does not currently exist on the system.
onBeforeRoomCreate	A gear is attempting to create a room on the system.
onAfterRoomCreate	A room has been successfully created on the system. The only valid response is PASS with no modification to the original stanza.
onServiceDiscoInfo	An entity has sent a disco#info packet to the TC service. The only valid response is PASS.
onServiceReconfig	The TC service receives a signal to reconfigure itself. The only valid response is PASS. This is a notification event only. The XDB packet will be of a type="set". The external component should not respond to this packet.
onDestroy	A room owner closes a room. The only valid response is PASS.
onClose	A gear requests to close a room.
onPacket	A new XML stanza is directed at a room, or participant within a room.
onMetaInfoGet	Room configuration information is available. The only valid response is PASS.
onBeforeMetaInfoSet	A room configuration is about to be modified by a user.
onAfterMetaInfoSet	A room configuration has been modified by a user. The only valid response is PASS with nothing in it.
onExamineRoom	A Jabber entity requests information, either by browse or disco, from a room. The only valid response is PASS.
onBeforeChangeUser	A change has been requested of a user role, nickname, or presence. This includes on entry, exit, nick change, availability change, or any role change (granting or revoking voice, moderator privilege).
onAfterChangeUser	A user has changed. The only valid response is PASS with nothing in it.
onBeforeChangeAffiliation	A user affiliation is about to change.

Event	Description
onAfterChangeAffiliation	A user affiliation has changed. The only valid response is PASS with nothing in it.
onBeforeRemoveAffiliation	A user affiliation is about to be removed.
onAfterRemoveAffiliation	A user affiliation has been removed. The only valid response is PASS with no modification to the original stanza.
onBeforeJoin	A user is about to join a room.
onAfterJoin	A user has joined a room. The only valid response is PASS with nothing in it.
onLeave	A user has left a room. The only valid response is PASS.
onBeforeSubject	A room subject is about to change.
onAfterSubject	A room subject has changed. The only valid response is PASS with nothing in it.
onBeforeInvite	A user is about to be invited to a room.
onAfterInvite	A user has been invited to a room. The only valid response is PASS with nothing in it.
onHistory	A room's history has been requested. The only valid response is PASS.
onBeforeSend	A message is about to be sent in a room.
onBeforeBroadcast	A message is about to be broadcast in a room.

Table 4: TC Parameters

Parameter	Description
Handling	Select **bounce** if errors returned from the compliance server should be bounced back to the originating party or component Select **pass** if they should be discarded.
Fire and Forget	Leave the check box unchecked if the IM and Presence Service node must wait for a response from the compliance server before it continues to process the event. Check the check box if the IM and Presence Service node does not require a response from the compliance server before it continues to process the event further.

If the same compliance profile is assigned to more than one compliance server, events are load balanced across each of the compliance servers. This reduces the load on individual compliance servers. Events are routed using an algorithm that ensures that related events are routed to the same compliance server. For one to one IMs, events are routed based on the combination of the to/from address, regardless of the packet's direction. This means that the full conversation between two users is routed to one compliance server. For group chat, events for a given chat room are routed using the chat room address, so that all events for a room are routed to one compliance server.

A system default profile is available in the system after fresh install or upgrade. This profile is called SystemDefaultComplianceProfile and cannot be deleted or modified. You can assign and unassign this profile as with any other.

The SystemDefaultComplianceProfile profile has four JSM and five TC events configured. If this profile is assigned, when any of its events occur in an IM and Presence Service cluster, they are passed on to the compliance server for handling, and a response is expected. The IM and Presence Service node handles the events based on the response from the compliance server. These events are previewed in read-only format if the SystemDefaultComplianceProfile is selected from the list of available compliance profiles.

Table 5: SystemDefaultComplianceProfile Pre-Configured Events

JSM Events	TC Events
e_SESSION	onBeforeInvite
es_END	onBeforeJoin
es_IN (for message stanzas only)	onBeforeRoomCreate
es_OUT (for message stanzas only)	onBeforeSend
	onLeave

If the same event(s) are configured in multiple profiles and these profiles are assigned to different third-party compliance servers, the events are handled in order as specified by routing priority. By default, routing priority of all profiles is defined by the order in which the profiles were added to the system. The routing priority can be re-configured.

Configure Compliance Profiles

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Compliance** > **Compliance Profiles**.

Step 2 Choose Add New.

Step 3 Enter a Name for the compliance profile.
Only alphanumeric characters are allowed. Spaces are not permitted.

Note The compliance profile name cannot be modified if the compliance profile is assigned to a compliance server.

Step 4 Enter a Description for the compliance profile.
This field is optional and should contain a meaningful description of the purpose of the compliance profile.

Step 5 Choose a JSM or TC event.

Step 6 For a JSM event, choose a Packet Type.
You cannot configure the same event with the same packet type more than once.

If you choose All, you cannot configure that same event with any other packet type, or vice versa.

Configuring the same JSM event with all packet types is the same as configuring one JSM event with packet type All.

Step 7 Choose a Handling type.

Step 8 Check the Fire and Forget check box to have the event handled by the compliance server outside of the IM and Presence Service event handling chain. IM and Presence Service continues to process the event regardless of the compliance server's handling.
By default, events are processed as part of the event handling chain and IM and Presence Service waits for a response from the compliance server.

If an event is processed as part of the event handling chain, and the compliance server responds with HANDLE, the event is not processed further by IM and Presence Service. If the compliance server responds with PASS, IM and Presence Service continues to process the event.

Step 9 To add additional events of either type, select Add New Event.

Troubleshooting Tip

If you update settings for events in a profile that is assigned to a third-party compliance server, you must restart the XCP Router service.

What to Do Next

When there is more than one compliance profile assigned and some or all of the events from one profile exist in the other profile(s), you can configure routing priority.

Related Topics

Compliance Profiles Routing Priority, on page 23

Compliance Profiles Routing Priority

You can configure routing priority when there is more than one compliance profile assigned and some or all of the events from one profile exist in the other profile(s). If each compliance profile has different events configured, routing priority is not applicable.

The default routing priority of the profiles configured in the system is the order in which they were configured.

Example

The following is an example of when you would use compliance profiles routing priority:

You have a compliance profile configured for events subject to Ethical Wall scrutiny, and another for the same events subject to IM logging. Each is assigned to a different compliance server. If you want the events subject to Ethical Wall scrutiny to be routed to the Ethical Wall server before being logged in the IM logging server, you must assign the Ethical Wall compliance profile the higher priority.

Configure Compliance Profile Routing Priority

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Compliance** > **Compliance Profiles Routing Priority**.

Step 2 In the **Compliance Profiles listed by routing priority (Top is highest priority)** window, use the up and down arrows to arrange the routing priority for your compliance profiles.

What to Do Next

You must restart the Cisco XCP Router service if the profiles to which you changed the routing priority are assigned. Follow the warning messages displayed to guide you as to when the router restart is needed.

Related Topics

Restart Cisco XCP Router Service, on page 11

Assigning Compliance Profiles to Compliance Servers

In IM and Presence Service 10.0.(1), all nodes in a cluster are subject to compliance unless you are upgrading from a system that had compliance previously configured. This means that although you can assign multiple compliance servers to your IM and Presence Service nodes, you do not need to assign one to every IM and Presence Service node for it to be subject to compliance.

Each compliance server in your cluster can be configured to process a different set of events. These sets of events are configured in compliance profiles, which are then assigned to compliance servers and IM and Presence Service nodes.

A system default profile is available in the system after fresh install or upgrade. This profile is called SystemDefaultComplianceProfile and cannot be deleted or modified. You can assign and unassign this profile as with any other. Until you create your own custom compliance profiles, you will only have the system default compliance profile available in the drop-down menu.

If you are upgrading from pre-10.0(1), your previous assignments have the SystemDefaultComplianceProfile assigned to them. This is the only profile available in the drop-down menu. The events in this default profile are the same events as were on the system prior to upgrading.

In previous releases, IM compliance worked on a per node basis. Every node with a compliance server assigned to it logged IM events to the compliance server only if those events were generated by that node. In this release, IM compliance works on a cluster basis. Regardless of how many or which nodes in a cluster have third party compliance server assigned, all nodes in the cluster are subject to compliance. Any event generated by any node in the cluster is logged to one of the compliance servers.

If you are upgrading from pre-10.0(1), your system continues working on a per node basis after the upgrade, but you can enable compliance logging for all nodes in the cluster. If you choose to do so, you will be able to create, update, and delete assignments, as well as change the compliance profiles to the custom compliance profiles that you created in your system.

Note It is not mandatory to enable compliance logging for all nodes on a system that had compliance previously configured. You can choose to retain compliance logging on a per node basis. In this case, you are only able to use the SystemDefaultComplianceProfile with your compliance server(s).

Assign Third-Party Compliance Server to IM and Presence Service Node

Before You Begin

Configure a third-party compliance server on IM and Presence Service.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Compliance** > **Compliance Settings**.

Step 2 Choose Third-Party Compliance Server from the Compliance Server Selection.

Step 3 Assign the third-party compliance server(s) to the IM and Presence Service nodes.

Note The same node cannot be assigned to multiple compliance servers if you have upgraded from a system that had compliance configured prior to the upgrade. In this case, if you want to be able to assign the same node to multiple compliance servers, you must enable compliance for the whole cluster.

The Open-port Component Name field is auto-generated based on the values in the first two columns. This is used when you configure the open-port component.

Step 4 Assign a compliance profile to each compliance server.
The same compliance profile can be assigned multiple times.

Note If you have upgraded your system from pre-10.0(1), and you configured compliance prior to the upgrade, only the system default profile is available in the drop-down menu. To use custom profiles, you must enable compliance for the whole cluster.

Step 5 Click Save.

Step 6 Restart the Cisco XCP Router service on all nodes if compliance is applied on all nodes in the cluster. Otherwise, it is sufficient to restart the Cisco XCP Router service on those nodes where you configured compliance.

Troubleshooting Tips

If you switch between IM compliance deployment options (for example, switch from the Message Archiver option to the Third-Party Compliance Server option), you must restart the Cisco XCP Router service. Note that you lose your third-party compliance settings if you switch between options.

Related Topics

Configure Third-Party Compliance Server on IM and Presence Service, on page 17
Restart Cisco XCP Router Service, on page 11
Configure Compliance Profiles, on page 22

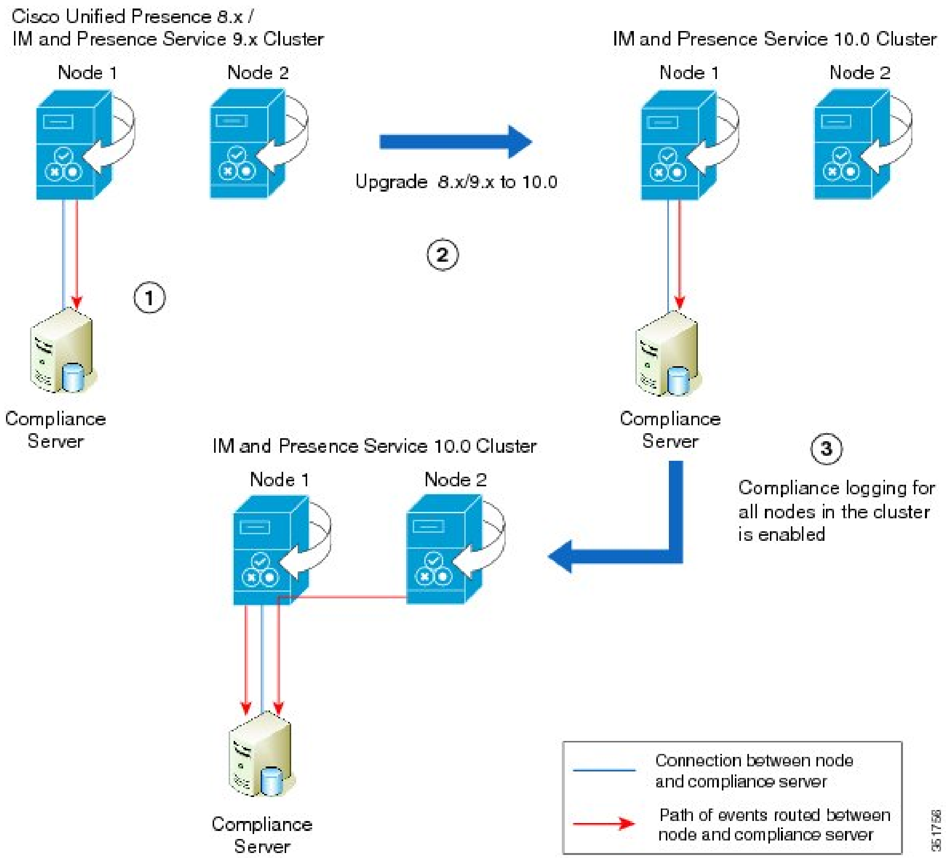
Enable Compliance Logging for all Nodes Following Upgrade, on page 29

Upgrade Scenarios

This section contains some sample upgrade scenarios that administrators who currently have compliance configured may find useful before upgrading to IM and Presence Service 10.0.(1).

Upgrade Scenario 1

Figure 4: Scenario 1

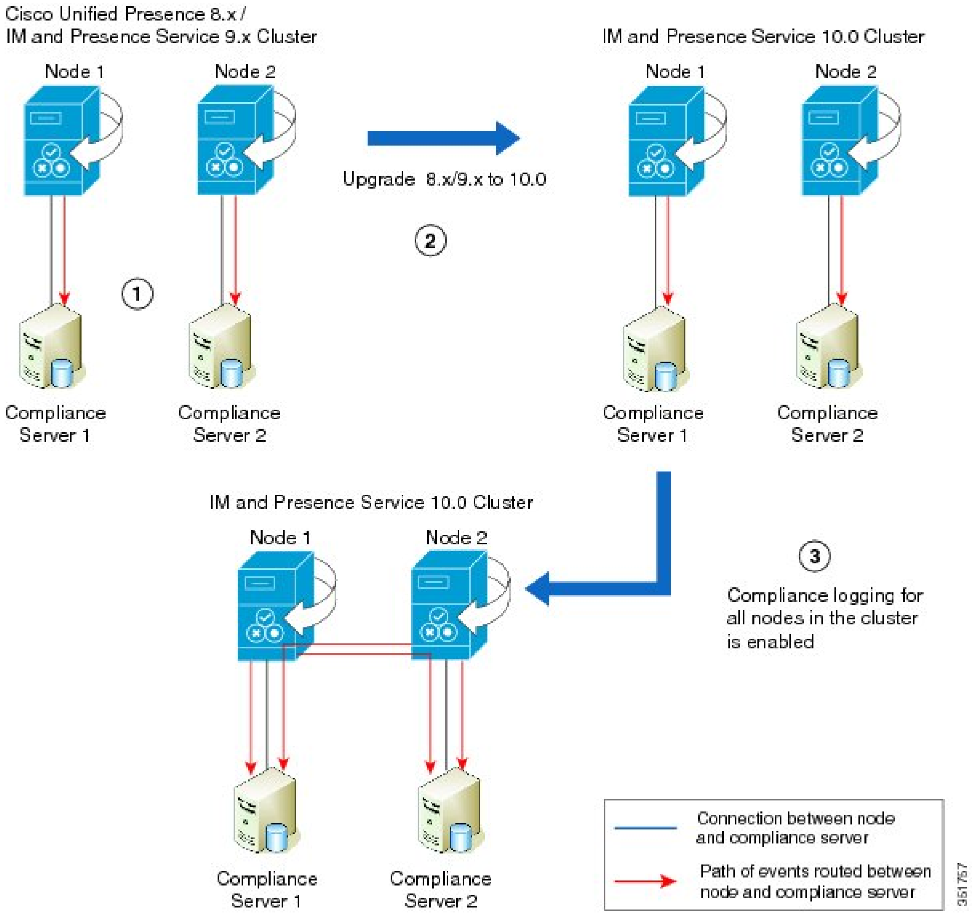

Cisco Unified Presence 8.x /
IM and Presence Service 9.x Cluster
Node 1
Node 2
Compliance Server
1
Upgrade 8.x/9.x to 10.0
2
IM and Presence Service 10.0 Cluster
Node 1
Node 2
Compliance Server
3
Compliance logging for all nodes in the cluster is enabled
IM and Presence Service 10.0 Cluster
Node 1
Node 2
Compliance Server
Connection between node and compliance server
Path of events routed between node and compliance server
351756

Stage 1	The cluster consists of two nodes and a compliance server. Node 1 is connected to the compliance server, and only events from this node are routed to the compliance server.
Stage 2	After the cluster has been upgraded to IM and Presence Service version 10.0, Node 1 maintains its connection to the compliance server and only events from this node are routed to the compliance server. Both Node 1 and the compliance server continue operation with no configuration changes required.

Stage 3	If compliance on the entire cluster is enabled by checking **Enable compliance logging for all nodes in the cluster** on the **Cisco Unified CM IM and Presence Administration > Messaging > Compliance > Compliance Settings** page, Node 1 will maintain its connection to the compliance server. The configuration on the compliance server will have to be updated to maintain operation. Events from both nodes will be routed to the compliance server via Node 1.

Upgrade Scenario 2

Figure 5: Scenario 2

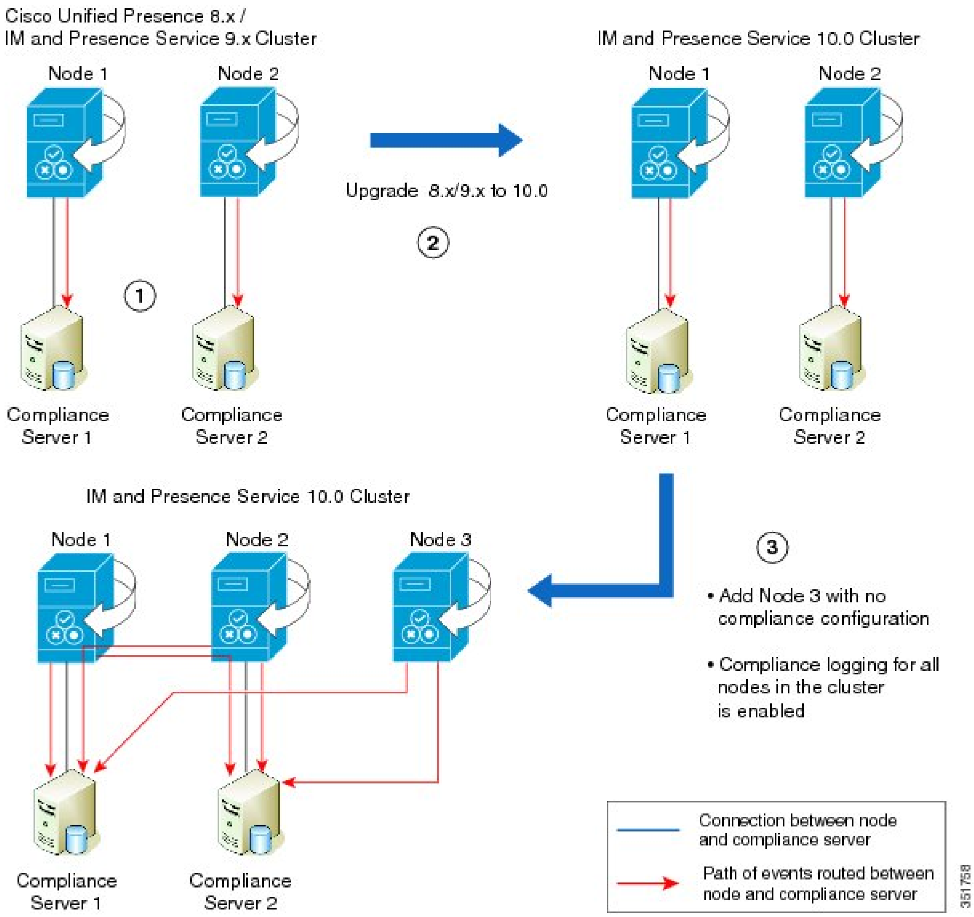

Cisco Unified Presence 8.x /
IM and Presence Service 9.x Cluster
Node 1
Node 2
Compliance Server 1
Compliance Server 2
1
Upgrade 8.x/9.x to 10.0
2
IM and Presence Service 10.0 Cluster
Node 1
Node 2
Compliance Server 1
Compliance Server 2
IM and Presence Service 10.0 Cluster
Node 1
Node 2
Compliance Server 1
Compliance Server 2
3
Compliance logging for all nodes in the cluster is enabled
Connection between node and compliance server
Path of events routed between node and compliance server
351757

Stage 1	The cluster consists of two nodes and two third-party compliance servers. Each node is connected, and each node routes events to their own respective compliance server.
Stage 2	After the cluster has been upgraded to IM and Presence Service version 10.0, each node is connected and each node routes events to their own respective compliance server. Both nodes and both of their respective compliance servers continue operation with no configuration changes required.

Stage 3	If compliance on the entire cluster is enabled by checking **Enable compliance logging for all nodes in the cluster** on the **Cisco Unified CM IM and Presence Administration > Messaging > Compliance > Compliance Settings** page, each node has a connection to its own compliance server. The configuration on the compliance servers will have to be updated to maintain operation. Events from Node 1 and Node 2 are routed to each compliance server.

Upgrade Scenario 3

Figure 6: Scenario 3


Cisco Unified Presence 8.x /
IM and Presence Service 9.x Cluster
Node 1
Node 2
Compliance Server 1
Compliance Server 2
1
Upgrade 8.x/9.x to 10.0
2
IM and Presence Service 10.0 Cluster
Node 1
Node 2
Compliance Server 1
Compliance Server 2
IM and Presence Service 10.0 Cluster
Node 1
Node 2
Node 3
Compliance Server 1
Compliance Server 2
3
• Add Node 3 with no compliance configuration
• Compliance logging for all nodes in the cluster is enabled
Connection between node and compliance server
Path of events routed between node and compliance server
351758

Stage 1	The cluster consists of two nodes and two third-party compliance servers. Each node is connected, and each node routes events to their own respective compliance server.
Stage 2	After the cluster has been upgraded to IM and Presence Service version 10.0, each node is connected and each node routes events to their own respective compliance server. Both nodes and both of their respective compliance servers continue operation with no configuration changes required.

Stage 3	On the upgraded IM and Presence Service version 10.0 cluster, an extra node with no compliance configuration is added, Node 3. If compliance on the entire cluster is then enabled by checking **Enable compliance logging for all nodes in the cluster** on the **Cisco Unified CM IM and Presence Administration > Messaging > Compliance > Compliance Settings** page, each node has a connection to its own compliance server. The configuration on the compliance servers will have to be updated to maintain operation. Events from Node 1 and Node 2 are routed to each compliance server. Events on Node 3 will be routed to both compliance servers via the open-ports on Node 1 and Node 2.

Enable Compliance Logging for all Nodes Following Upgrade

Caution When you enable this setting, you cannot change it back.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Compliance** > **Compliance Settings**.

Step 2 Choose Third-Party Compliance Server from the Compliance Server Selection.

Step 3 Check the **Enable compliance logging for all nodes in the cluster. Once enabled, this setting cannot be reverted back. Please refer to the documentation for optimal configuration** check box and click Save.
A warning message appears.

Step 4 Click OK.

Step 5 Restart the Cisco XCP Router service on all nodes in the cluster.

What to Do Next

After you enable compliance for all nodes, the component name used by IM and Presence Service changes to an auto-generated format. Update your compliance server(s) with the new component name to continue using the feature.

Related Topics

Restart Cisco XCP Router Service, on page 11

Third-Party Compliance Server Failure Event Handling

About Third-Party Compliance Server Failure Event Handling

This chapter describes the behavior IM and Presence Service users will experience when problems occur with compliance integration or during HA failover.

Note The sections in this chapter assume that compliance profiles include the following events (except where otherwise stated):

- e_SESSION (recording user logins)
- es_END (recording user logouts)
- es_OUT/es_IN for message (recording IM conversations)
- One or more TC events (recording chat room interactions)

Event handling during a Compliance Server or Service Outage

A Single Compliance Server or Service Shutdown

Assumed deployment:

- One or more IM and Presence Service node(s) deployed in a sub-cluster.
- One IM and Presence Service node is configured with a single third-party compliance server.

If the compliance server or service is shut down gracefully users will be affected as follows:

- Users will continue to log in and log out of IM and Presence Service using their XMPP clients as normal, but login and logout events will not be logged to the compliance server.
- Users will be blocked from sending IMs or interacting with chat rooms, and in each case users will receive a server error response.

A Single Compliance Server or Service Ungraceful Failure or Network Disruption

Assumed deployment:

- One or more IM and Presence Service node(s) deployed in a sub-cluster.
- One IM and Presence Service node is configured with a single third-party compliance server.

For an initial period of up to 5 minutes, if the compliance server or service fails ungracefully or if there is a disruption to the network between an IM and Presence Service node and the compliance server, the node will attempt to queue events for that compliance server. Individual events will be queued for 30 seconds before being processed or bounced.

After 5 minutes, if the compliance server or network has not recovered, the connection to the server will be dropped and events will no longer be queued. In this situation, events will be processed or bounced immediately. Users will be affected as follows:

- Users will experience up to 30 seconds delay on logging in to IM and Presence Service, but there will be no delay when logging out. Login and logout events will not be logged to the compliance server.
- Users will be blocked from sending IMs or interacting with chat rooms. In each case users will receive a server error response, but there may be a delay of up to 30 seconds before the error is received.

- Users may experience delays of up to 30 seconds while presence status updates are being processed.

Compliance Server or Service Graceful Outage with Multiple Compliance Servers

Assumed deployment:

- One IM and Presence Service node deployed in a sub-cluster.
- One IM and Presence Service node is configured with multiple third-party compliance servers.

Where an IM and Presence Service node is connected to multiple compliance servers, normal behavior is for events to be load-balanced across the compliance servers using a JID-based algorithm. Events for different users may be routed to different compliance servers.

If one of the compliance servers or services is shut down gracefully, then events that would have been routed to that server will instead be routed to the remaining compliance server(s).

Compliance Server or Service Ungraceful Outage with Multiple Compliance Servers

Assumed deployment:

- One IM and Presence Service node deployed in a sub-cluster.
- One IM and Presence Service node is configured with multiple third-party compliance servers.

Where an IM and Presence Service node is connected to multiple compliance servers, normal behavior is for events to be load-balanced across the compliance servers using a JID-based algorithm. Events for different users may be routed to different compliance servers.

If one of the compliance servers or services fails ungracefully, or if there is a disruption to the network between an IM and Presence Service node and that server, then users will be affected as follows:

- Some users will experience up to 30 seconds delay in logging in to IM and Presence Service, but there will be no delay when logging out. Login and logout events will not be logged to the compliance server.
- Some users will be blocked from sending IMs or interacting with chat rooms for a period of up to 5 minutes. After this period, affected users can continue to send IMs or interact with chat rooms, and the events will be routed to one of the remaining compliance servers.
- Some users may experience delays of up to 30 seconds for presence status updates to be processed.

Compliance Server or Service Outage with Multiple Compliance Servers and Profiles

Where an IM and Presence Service node is configured to connect to multiple compliance servers, each of which uses a different compliance profile, and the profiles contain one or more identical events, normal behavior is for these events to be routed in turn to the compliance server associated with each compliance profile according to each profile's priority.

This behavior is explained in more detail in the following example:

Assumed deployment:

- One IM and Presence Service node deployed in a sub-cluster with multiple profiles containing one or more identical events.

- The IM and Presence Service node is configured with multiple third-party compliance servers and profiles.

Each compliance profile has the following events configured:

Profile 1:

- e_SESSION (recording user logins)
- es_OUT/es_IN for message (recording IM conversations)
- es_END (recording user logouts)

Profile 2:

- es_OUT/es_IN for message (recording IM conversations)

Profile assignments:

- Profile 1 is assigned to Compliance Server 1
- Profile 2 is assigned to Compliance Server 2
- Profile 1 has the highest priority

During normal behavior:

When a user sends an IM, the es_OUT event for Profile 1 is routed to Compliance Server 1. When Compliance Server 1 acknowledges the event, the es_OUT event for Profile 2 is routed to Compliance Server 2.

If Compliance Server 1 experiences an ungraceful outage then the following sequence will take place:

1. User A sends IM to user B.
2. The es_OUT event (Profile 1) is queued for Compliance Server 1.
3. The es_OUT event (Profile 1) times out after 30 seconds.
4. The es_OUT event (Profile 1) is bounced, and the IM sender receives an error response.
5. The es_OUT (Profile 2) event is not processed and the event is not sent to Compliance Server 2.

In this case users will be affected as follows:

- Users will be blocked from sending IMs. Users will receive a server error response in each case, but there may be a delay of up to 30 seconds before the error is received. Events associated with the IM conversation will not be routed to the remaining compliance servers.
- Users may experience delays of up to 30 seconds for presence status updates to be processed.

Compliance Handling During an IM and Presence Service Node Failure

Compliance Handling during Manual Node Failover

Assumed deployment:

- Two IM and Presence Service nodes deployed in a sub-cluster with HA enabled.

- Each IM and Presence Service node is configured with a different third-party compliance server using the same compliance profile.

During normal behavior:

- Events are load-balanced across the compliance servers using a JID-based algorithm.
- Events for different users may be routed to different compliance servers.
- Events routed to a compliance server are routed via the IM and Presence Service node to which it is connected.

If an IM and Presence Service node manual failover occurs, events normally routed to its associated compliance server will be handled as follows:

- Login and logout events will not be logged to the compliance server. Some users will experience a delay of up to 30 seconds when logging in to IM and Presence Service, but there will be no delay when logging out.
- During failover, some users will be blocked from sending IMs or interacting with chat rooms. In this case users will receive a server error response in each case, but there may be a delay of up to 30 seconds before the error is received. Events which are blocked will not be logged to the compliance server.
- When failover has been completed, IM or group chat events will be processed by the compliance server connected to the other IM and Presence Service node and stanzas will be delivered normally.

Compliance Handling during Automated Node Failover

Assumed deployment:

- Two IM and Presence Service nodes deployed in a sub-cluster with HA enabled.
- Each IM and Presence Service node is configured with a different compliance server using the same compliance profile.

During normal behavior:

- Events are load-balanced across the compliance servers using a JID-based algorithm.
- Events for different users may be routed to different compliance servers.
- Events routed to each compliance server are routed via the IM and Presence Service node to which it is connected.

Note If the failover is not caused by a failure or shutdown of the Cisco XCP Router service, compliance events will continue to be routed to the compliance servers as normal. Events routed to the compliance server connected to the IM and Presence Service node that has failed over will continue to be routed to the compliance server.

Compliance Handling during Network Outage Between Multiple Nodes

Assumed deployment:

- Two IM and Presence Service nodes deployed in a sub-cluster with HA enabled.
- Each IM and Presence Service node is configured with a different compliance server using the same compliance profile.

During normal behavior:

- Events are load-balanced across the compliance servers using a JID-based algorithm.
- Events for different users may be routed to different compliance servers.
- Events routed to each compliance server are routed via the IM and Presence Service node to which it is connected.

If a network outage between the IM and Presence Service nodes occurs, events for users that are normally routed to the compliance server associated with the other IM and Presence Service node will be handled as follows:

- Some users will experience a delay of up to 30 seconds when logging in to IM and Presence Service, but there will be no delay when logging out. Login and logout events will not be logged to the compliance server.
- During the outage, some users will be blocked from sending IMs or interacting with chat rooms. Users will receive a server error response in each case, but there may be a delay of up to 30 seconds before the error is received. Events which are blocked will not be logged to the compliance server.
- If the outage continues for longer than 2 minutes, events will be processed by another compliance server in the deployment and stanzas will be delivered normally.

Compliance Handling during Cisco XCP Router Service Failure

Assumed deployment:

- Two IM and Presence Service nodes deployed in a sub-cluster with HA not enabled.
- Each IM and Presence Service node is configured with a different compliance server using the same compliance profile.

Note In this section, consequences when HA is enabled will also be highlighted.

During normal behavior:

- Events are load-balanced across the compliance servers using a JID-based algorithm.
- Events for different users may be routed to different compliance servers.
- Events routed to each compliance server are routed via the IM and Presence Service node to which it is connected.

The difference in effects that users will experience when HA is either enabled or not enabled are as follows:

- When HA is enabled users will remain logged in and will be moved to the remaining node.
- When HA is not enabled, users on the failed node will be logged out and will not get any service.

More general effects include:

- Events normally routed to the compliance server connected to the failed IM and Presence Service node, will be routed to the compliance server connected to the other IM and Presence Service node.
- If the failure is transient, some users will initially be blocked from sending IMs or interacting with chat rooms. Users will receive a server error response in each case, but there may be a delay of up to 30 seconds before the error is received. Events which are blocked will not be logged to the compliance server.
- If the failure lasts for a longer period, IMs will be processed normally and be routed to the compliance server connected to the other IM and Presence Service node.

IM and Presence Service Node and Third-Party Compliance Server Alarm

When an IM and Presence Service node is integrated with a third-party compliance server, messages will only be delivered to users after it successfully logs the message to the third-party compliance server.

If an IM and Presence Service node loses its connection to the third-party compliance server to which it is directly connected, IM and Presence Service does not deliver the message to the recipient.

To ensure that you are notified if this connection is lost, you should verify that its associated alarm settings are properly configured.

Procedure

Step 1 Sign into IM and Presence Service.

Step 2 Choose **Cisco Unified IM and Presence Serviceability** > **Alarm** > **Configuration**.

Step 3 Choose the server for which you want to configure the alarm from the Server drop down menu, and click **Go**.

Step 4 Choose IM and Presence Services from the Service Group drop down menu, and click **Go**.

Step 5 Choose Cisco XCP Router from the Service drop down menu, and click **Go**.

Step 6 Configure the alarm settings as preferred.

Step 7 Click **Save**.

Third-Party Compliance Server Troubleshooting

If the compliance integration is not operating as expected and you are experiencing problems such as:

- Slow user login
- Blocked IMs
- Blocked group chat events when IM and Presence Service is configured to use third-party compliance.

Then carry out the following list of checks to troubleshoot the compliance integration:

1. Check the Troubleshooter in the Compliance Server Settings window. If the Troubleshooter is red continue with step 2. If the troubleshooter is green go to step 3.
2. Check the connection settings for the third-party compliance server in the third-party compliance server settings window.
3. To verify that the Cisco XCP Router service has established a connection to the third-party compliance server, check the Cisco XCP Router service logs using RTMT. Scan the logs for entries such as the following:

    - `Component op-gwydlvm131.gwydlvm1153-cisco-com is CONNECTED`

      This entry shows that the Cisco XCP Router service has established a network connection to the third-party compliance server.

    - `Component op-gwydlvm131.gwydlvm1153-cisco-com is ACTIVE`

      This entry shows that the Cisco XCP Router service and the third-party compliance server have completed authentication.

4. If the logs show `CONNECTED` but not `ACTIVE`, verify that:

    - The correct password has been configured on IM and Presence Service and on the third-party compliance server.
    - The correct component name has been configured on the third-party compliance server.

    If the Cisco XCP Router service is unable to connect to the third-party compliance server, the Cisco XCP Router service logs will show output similar to the following:

    ```
    Connecting on fd 22 to host '10.53.52.205', port 7999
    Unable to connect to host '10.53.52.205', port 7999:(111) Connection refused
    Component op-gwydlvm131.gwydlvm1153-cisco-com is GONE
    ```

5. If the Cisco XCP Router Service is unable to establish a connection to the third-party compliance server, check that:

    - The correct IP/FQDN and port have been configured on IM and Presence Service and on the third-party compliance server.
    - The third-party compliance server is running and listening on the specified port.

6. If the logs show `CONNECTED` and `ACTIVE` when IM and Presence Service passes events to the compliance server for processing, the third-party compliance server must respond to each event before IM and Presence Service can continue to process the event. If you suspect that the compliance server is not responding, check the compliance server logs.