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

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

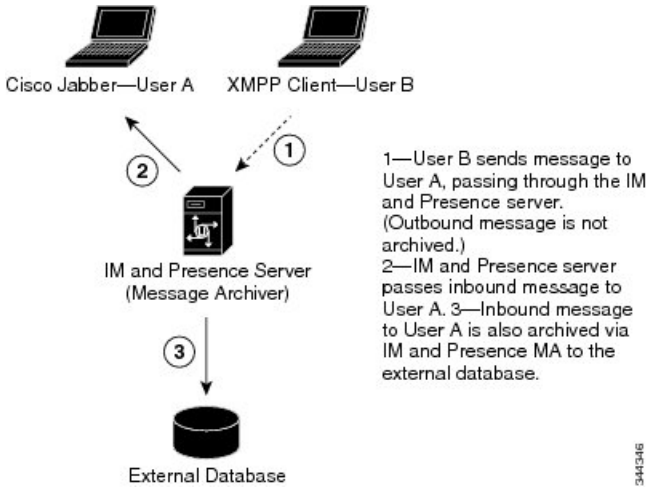
When using IM compliance in a single cluster, we highly recommend that you deploy one external database per cluster to which all incoming messages sent to users in the cluster are logged.

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

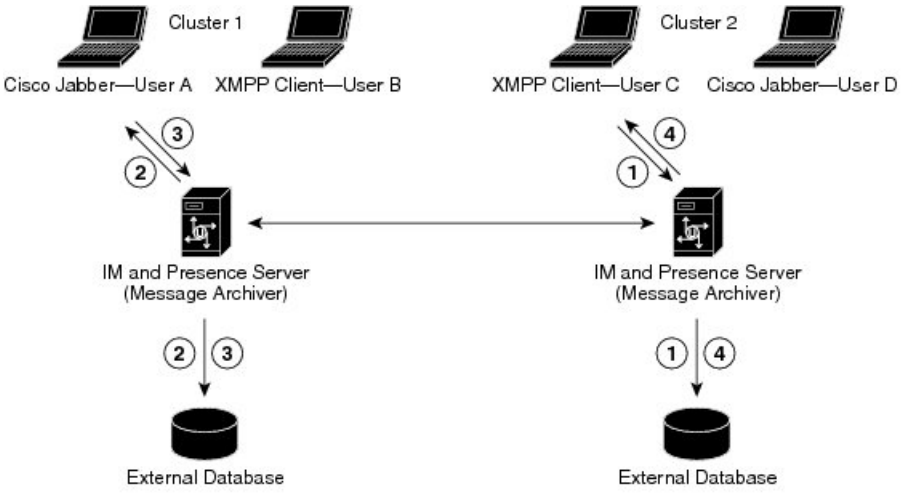


Intercluster or Federated Network Configuration

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



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';