External Database Requirements

This guide provides information about how to configure an external database for Cisco Unified Communications Manager IM and Presence Service features. The following features require an external database:

- Persistent Group Chat
- High Availability for Persistent Chat
- Message Archiver (IM Compliance)
- Managed File Transfer

- How to use this Guide, on page 1
- External Database Setup Requirements, on page 2
- Additional Documentation, on page 3
- External Database Setup Prerequisites, on page 4
- Performance Considerations, on page 4
- About Security Recommendations, on page 5

How to use this Guide

Refer to the following chapters for instructions on how to configure your external database.

Procedure

	Command or Action	Purpose
Step 1	External Database Requirements, on page 1	Review support information and other requirements for your external database.
Step 2	Install the external database: • Install PostgreSQL • Install Oracle • Install Microsoft SQL Server	Refer to one of the chapters on the left for installation information.
Step 3	Configure IM and Presence Service for External Database	Configure the IM and Presence Service for the external database connection.

What to do next

After setting up the external database, refer to the additional material in this guide for information on administering your external database.

External Database Setup Requirements

General Requirements

Cisco suggests having a certified PostgreSQL, Oracle, or Microsoft SQL Server administrator to maintain and retrieve information from the external database.

Hardware and Networking Requirements

- The external database should be installed on a dedicated server. The database can be deployed on virtualized or non-virtualized platforms.
- See the vendor database documentation for details on supported operating systems and platform requirements.
- IPv4 and IPv6 are supported by IM and Presence Service.

Software Requirements

The following table contains general external database support information for the IM and Presence Service. For detailed information specific to IM and Presence features, refer to the subsequent "Feature Requirements" section.

Table 1: Database Support for the IM and Presence Service

Database	Supported Versions
PostgreSQL	**Note** PostgreSQL 12.x and higher are compatible only with IM and Presence Service Release, 12.5(1) SU6 and higher. All currently active PostgreSQL versions from 12.x through 16.x are supported. Now, validation was performed against versions 12.x, 13.x and 16.x.
Oracle	Testing is performed using Oracle 9g, 10g, 11g, 12c, and 19c versions. Since the IM and Presence features are using common Oracle features such as basic SQL statements, Stored Procedures, and basic indexing; we expect that future versions remain compatible and will be supported unless otherwise specified in this document. Cisco plans to include compatibility testing of newer major Oracle DB releases during future major IM and Presence releases.
Microsoft SQL Server	All currently active MS SQL versions from 2016 through 2022 are supported. Now, validation was performed against versions 2016, 2017, 2019, and 2022.

Feature Requirements

IM and Presence Service features which depend on the integration with an external database support Oracle, PostgreSQL, and Microsoft SQL Server as external databases. External database requirements differ depending on which features you want to deploy on the IM and Presence Service. See the following table for support information for specific IM and Presence Service features.

Table 2: External Database Requirements for Specific IM and Presence Service Features

Feature	Requirements
Persistent Group Chat feature	A minimum of one unique logical external database instance (tablespace) is required for the entire IM and Presence Service intercluster. A unique logical external database instance for each IM and Presence Service node or redundancy group in an IM and Presence Service cluster will provide optimum performance and scalability, but is not mandatory.
High Availability for Persistent Chat feature	Make sure that both presence redundancy group nodes are assigned to the same unique logical external database instance. Cisco does not provide detailed back-end database support. You are responsible for resolving back-end database issues on your own.
Message Archiver (compliance) feature	We highly recommend that you configure at least one external database for each IM and Presence Service cluster; however you may require more than one external database for a cluster depending on your database server capacity.
Managed File Transfer feature	You require one unique logical external database instance for each IM and Presence Service node in an IM and Presence Service cluster. **Note** Database table space can be shared across multiple nodes or clusters provided capacity and performance isn't overloaded.

Note If you deploy any combination of the persistent group chat, message archiver (compliance), and managed file transfer features on an IM and Presence Service node, the same unique logical external database instance (tablespace) can be shared across the features as each feature uses separate data tables. This depends on the capacity of the database instance.

Additional Documentation

This procedure only describes how to configure the external database on the IM and Presence Service. It does not describe how to fully configure the features that require an external database. See the documentation specific to the feature you are deploying for the complete configuration:

- For information on configuring the message archiver (compliance) feature on the IM and Presence Service, see *Instant Messaging Compliance for IM and Presence Service.*
- For information on configuring the persistent group chat feature on the IM and Presence Service, see *Configuration and Administration of the IM and Presence Service.*

- For information on configuring the managed file transfer feature on the IM and Presence Service, see *Configuration and Administration of the IM and Presence Service* .

External Database Setup Prerequisites

Before you install and configure the external database on the IM and Presence Service, perform the following tasks:

- Install the IM and Presence Service nodes as described in *Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service*.
- Configure the IM and Presence Service nodes as described in *Configuration and Administration of IM and Presence Service*.

Caution If the IM and Presence Service connects to an external database server using IPv6, ensure that the enterprise parameter is configured for IPv6 and that Eth0 is set for IPv6 on each node in the deployment; otherwise, the connection to the external database server fails. The message archiver and Cisco XCP Text Conference Manager will be unable to connect to the external database and will fail. For information about configuring IPv6 on the IM and Presence Service, see *Configuration and Administration of IM and Presence Service*.

Performance Considerations

When you configure an external database with the IM and Presence Service, you must consider the following recommendations:

- Reduce the round-trip delay (RTT) between the IM and Presence Service cluster and the external database to avoid performance issues. This is normally accomplished by locating the external database server as close as possible to the IM and Presence Service cluster.
- Do not allow the external database entries to be full which causes performance issues on the IM and Presence Service cluster. Regular maintenance of the external database plays an important role in preventing IM and Presence Service performance degradation.

Note The external database maintenance further tunes the query execution mechanisms of the database engine itself when the number of records in the database reaches certain threshold.

For example, on the MSSQL database by default when you enable the query execution optimization mechanism that is called Parameter Sniffing, it can negatively affect the performance of persistent chat service. If this optimization mechanism does not adjust with plan guides for concrete IM and Presence Service queries, delay in Instant Messages delivery to persistent chats will be introduced.

Related Topics

PostgreSQL documentation
Oracle documentation
Microsoft Server documentation

About Security Recommendations

External Database Connection Security

The IM and Presence Service provides a secure TLS/SSL connection to the external database but only when Oracle or Microsoft SQL Server is chosen as the database type. We recommend that you consider this security limitation when you plan your IM and Presence Service deployment, and consider the security recommendations we provide in this topic.

Maximum Limit Connection Setup

For additional security, you can limit the maximum number of permitted connections to the external database. Use the guideline we provide here to calculate the number of database connections that are appropriate for your deployment. This section is optional configuration. The guideline infers that:

- You are running the managed file transfer, message archiver (compliance), and persistent group chat features on the IM and Presence Service.
- You configure the default number of connections to the database for the persistent group chat feature on the **Cisco Unified CM IM and Presence Administration** interface.

Guideline

PostgreSQL — max_connections = (N ×15) + Additional Connections

Oracle — QUEUESIZE = (N ×15) + Additional Connections

Microsoft SQL Server — the maximum number of concurrent connections = (N x15) + Additional Connections

- N is the number of nodes in your IM and Presence Service cluster.
- 15 is the default number of connections to the database on the IM and Presence Service, that is, five connections each for the managed file transfer, message archiver, and persistent group chat features.
- Additional Connections represents any independent administration or database administrator (DBA) connections to the database server.

PostgreSQL

To limit the number of PostgreSQL database connections, configure the `max_connections` value in the `postgresql.conf file` located in the *`install_dir`*`/data` directory. We recommend that you set the value of the `max_connections` parameter equal to, or slightly larger than, the above guideline.

For example, if you have an IM and Presence Service cluster containing six nodes, and you require an additional three DBA connections, using the guideline above, you set the max_connections value to 93.

Oracle

To limit the number of Oracle database connections, configure the QUEUESIZE parameter in the listener.ora file located in the *`install_dir`*`/data` directory. We recommend that you set the value of the QUEUESIZE parameter equal to the above guideline.

For example, if you have an IM and Presence Service cluster containing 4 nodes, and you require one additional DBA connection, using the guideline above, you set the QUEUESIZE value to 61.

Microsoft SQL Server

To limit the number of MS SQL Server database simultaneous connections carry out the steps below. We recommend that you set the size of the queue equal to the above guideline.

1. From the **SQL Server Configuration Manager**, right-click the node you want to configure and click **Properties**.
2. Click **Connections**.
3. In the **Connections** pane, enter a value from 0 to 32767 in the **Max number of concurrent connections** dialog box.
4. Restart the Microsoft SQL Server.

Default Listener Port Setup

Note This section is an optional configuration.

For additional security, you may choose to change the default listening port on the external database:

- For PostgreSQL, see Set Up PostgreSQL Listening Port for details on how to edit the default listener port.
- For Oracle, you can edit the default listener port by editing the `listener.ora` config file
- For Microsoft SQL Server, you can assign a TCP/IP port number as the default listener port in the SQL Server Configuration Manager. For details, see Default Listener Port Setup for Microsoft SQL Server.