Configure IM and Presence Service for External Database

This chapter provides information about configuring the IM and Presence Service for the external database connection.

About External Database Assignment

External Database and Node Assignment

When you configure an external database entry on the IM and Presence Service, you assign the external database to a node, or nodes, in your cluster as follows:

- Message Archiver (compliance) — You require at least one external database per cluster. Depending on your deployment requirements, you can also configure a unique external database per node.
- Persistent Group Chat — You require a unique external database per node. Configure and assign a unique external database for each node in your cluster.
- Managed File Transfer — You require one unique logical external database instance for each IM and Presence Service node, in an IM and Presence Service cluster/sub-cluster that has the Cisco XCP File Transfer Manager service activated.
- If you deploy the persistent group chat, message archiver, and managed file transfer features on an IM and Presence Service node, you can assign the same external database to all or any combination of the features.

For more information see:

- Message Archiver — *Instant Messaging Compliance for IM and Presence Service on Cisco Unified Communications Manager*.

- Persistent Group Chat — *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager.*
- Managed File Transfer — *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

Related Topics

Set Up External Database Entry on IM and Presence Service, on page 2
External Database Connection, on page 2

External Database Connection

IM and Presence Service does not establish a connection to the external database when you configure an external database entry. The external database has not created the database schema at this point. It is only when you assign an external database entry to a node that IM and Presence Service establishes an ODBC (Open Database Connectivity) connection with the external database. Once IM and Presence Service establishes a connection, the external database creates the database tables for the IM and Presence Service features.

Once you assign an external database entry to a node, you can validate the connection using the System Troubleshooter in the **Cisco Unified CM IM and Presence Service Administration** user interface.

Related Topics

Set Up External Database Entry on IM and Presence Service, on page 2
Verify External Database Connection Status on IM and Presence Service

Set Up External Database Entry on IM and Presence Service

Perform this configuration on the IM and Presence Service database publisher node of your cluster.

Caution If your IM and Presence Service node 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 are unable to connect to the external database and fail. For information about configuring IPv6 on IM and Presence Service, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

Before you begin

- Install and configure the external database.
- Obtain the hostname or IP address of the external database.
- If using Oracle, retrieve the tablespace value. To determine the tablespace available for your Oracle database, execute the following query as sysdba:

```
SELECT DEFAULT_TABLESPACE FROM DBA_USERS WHERE USERNAME = 'USER_NAME';
```

Note The user name must be capitalized and in single quotes (a string literal) for this command to succeed, even if you defined the user with lowercase characters.

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Messaging** > **External Server Setup** > **External Databases**.

Step 2 Click **Add New**.

Step 3 Enter the name of the database that you defined at external database installation, for example, **`tcmadb`**.

Step 4 Choose the database type from the drop-down list, Postgres, Oracle, or Microsoft SQL Server.

Step 5 If you chose Oracle as the database type, enter the tablespace value.

Step 6 Enter the username for the database user (owner) that you defined at external database installation, for example, **`tcuser`**.

Step 7 Enter and confirm the password for the database user, for example, **`mypassword`**.

Note The password length for external database should be less or equal to 30 characters long.

Step 8 Enter the hostname or IP address for the external database.

Step 9 Enter a port number for the external database.

The default port numbers for Postgres (5432), Oracle (1521), Oracle with SSL enabled (2484), and Microsoft SQL Server (1433) are prepopulated in the **Port Number** field. You can choose to enter a different port number if required.

Step 10 If you chose Oracle or Microsoft SQL Server as the Database Type the **Enable SSL** check box becomes active. Check the check box to enable SSL.

Note
- If you chose Microsoft SQL Server as the Database Type, the **Certificate Name** drop-down list remains inactive because all certificates in the cup-xmpp-trust list are used to verify the certificate sent from the Microsoft SQL Server
- If you chose Microsoft SQL Server as the Database Type, the hostname must match the entry in the **Common Name** field of the certificate presented by the SQL Server.

If you chose Oracle as the Database Type, the **Certificate Name** drop-down list becomes active. Choose a certificate from the drop-down list.

Note

- When the Enable SSL check box or the Certificate drop-down field is modified, a notification to restart the corresponding service assigned to the external database is sent. A message concerning either Cisco XCP Message Archiver or Cisco XCP Text Conference Manager will be generated.
- The certificate you need to enable SSL must be uploaded to the cup-xmpp-trust store. You must upload this certificate before you enable SSL.
- Once the certificate is uploaded to the cup-xmpp-trust store, you must wait 15 minutes for the certificate to propagate to all the nodes of the IM and Presence Service cluster. If you do not wait, the SSL connection on nodes where the certificate has not propagated fails.
- If the certificate is missing or has been deleted from the cup-xmpp-trust store, an alarm XCPExternalDatabaseCertificateNotFound is raised in the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT).

  Note No alarm is raised if the external database type chosen is Microsoft SQL Server.

- The following ciphers have been tested with Microsoft SQL Server:
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA256

Step 11 Click **Save**.

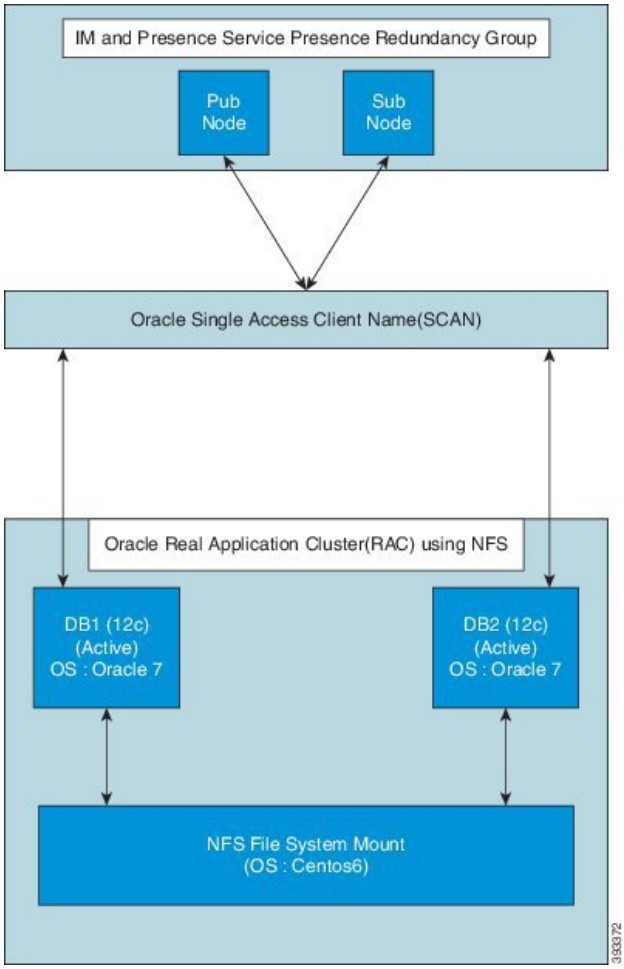
Related Topics

Verify External Database Connection, on page 7

External Database for Persistent Chat High Availability

For information on supported versions, refer to the External Database Setup Requirements section of the *Database Setup Guide for IM and Presence Service*.

Figure 1: Oracle High Availability Setup



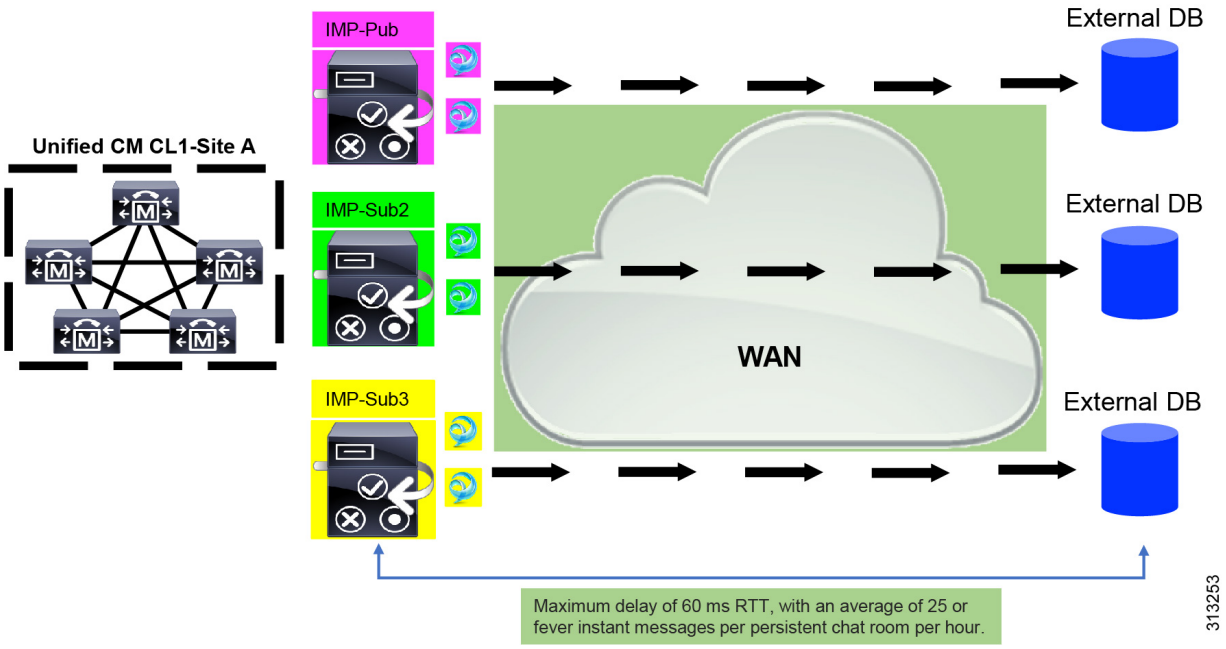
Message Archiver Network Latency

https://ciscoenterprise.acrolinx.cloud for the Acrolinx URL

Cisco IM and Presence Service is enabled for persistent chat, message archiving, or compliance logging. We recommend to place the external database servers on the same side of the WAN as the associated Cisco IM and Presence Service subclusters to keep a low network latency.

In case the external database cannot be located on the same side of the WAN as its associated Cisco IM and Presence Service subcluster, the following considerations apply with respect to deployment profile and latency.

Figure 2: Message Archiver with External Database Across the WAN

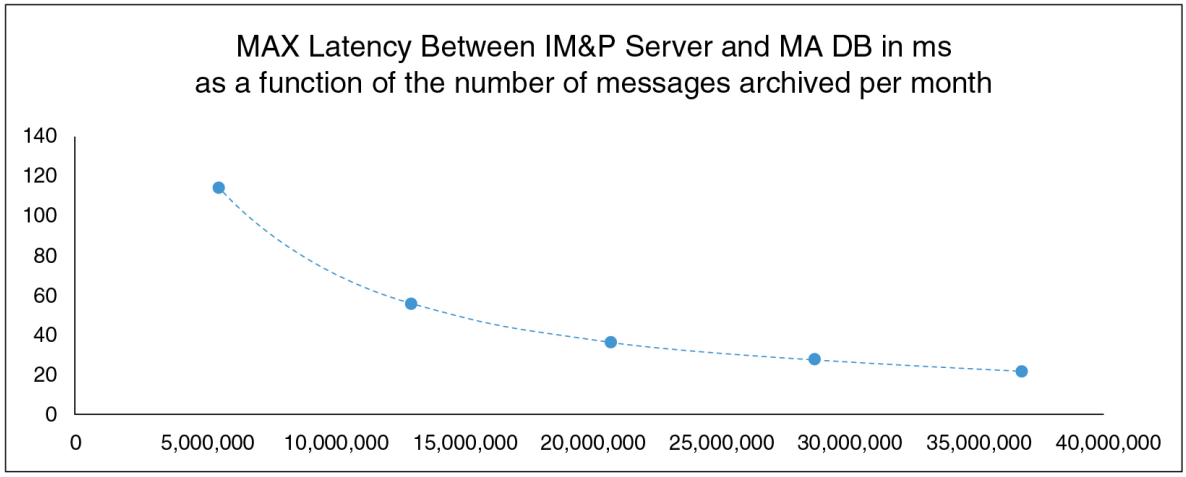


The Message Archiver feature is latency dependent. When modeling acceptable network latency due to round-trip time (RTT), the following parameters apply:

- Number of users per Cisco IM and Presence Service
- Average number of messages per time interval
- Number of active chat rooms
- Average number of users per active chat room
- Average number of messages per active chat room per time interval
- Average number of logged in devices per user

As network latency increases, the number of users, devices, and/or messages per user must decrease.

Figure 3: Max Latency/RTT plot



457667

Calculating the Max Latency/RTT

Use the guideline we provide here to calculate the Max Latency/RTT.

Guideline

The Max Latency/RTT time (in ms) for the given number of monthly archived messages is calculated using the following formula:

$$\text{Max RTT} = 8 * 10^{7} * \text{TMM}^{-0.867}$$

Where TMM represents the total number of archived messages per month.

Verify External Database Connection

If you make a configuration change in the `install_dir/data/pg_hba.conf` file or the `install_dir/data/postgresql.conf` file after you assign the external database, perform these steps:

Step 1 Unassign and reassign the external database to the IM and Presence Service node.

Step 2 Restart the Cisco XCP Router service. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Control Center - Network Services** to restart this service.

Related Topics

Install PostgreSQL
Install Oracle
Install Microsoft SQL Server

Verify External Database Connection Status on IM and Presence Service

IM and Presence Service provides the following status information on an external database:

- Database reachability — Verifies that the IM and Presence Service can ping an external database.
- Database connectivity — Verifies that the IM and Presence Service has successfully established an Open Database Connectivity (ODBC) connection with the external database.
- Database schema verification — Verifies that the external database schema is valid.

Caution If your IM and Presence Service node 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 (compliance) and Cisco XCP Text Conference Manager is unable to connect to the external database and fails. For information about configuring IPv6 on IM and Presence Service, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Messaging** > **External Server Setup** > **External Databases**.

Step 2 Click **Find**.

Step 3 Choose the external database entry that you want to view.

Step 4 Verify that there are check marks beside each of the result entries for the external database in the External Database Status section.

Step 5 In the **Cisco Unified CM IM and Presence Administration** user interface, choose **Diagnostics** > **System Troubleshooter**.

Step 6 Verify that there are check marks beside the status of each of the external database connection entries in the External Database Troubleshooter section.

Troubleshooting Tips

- The IM and Presence Service generates an alarm if it loses ODBC to an external database.
- Changing the password of the external database user when the IM and Presence Service is already connected to the external database will not affect the existing connections. When the Cisco XCP Router service is restarted, it destroys the existing connections and the new password is used for creating new connections.

  If the user password is changed only on the external database, the configured IM and Presence features relying on the external database continues to work using the existing connections established with the old user password. However, this transient phase shall be kept to a minimum and at the earliest ensure to update the password on the IM and Presence Service too.
- You can also verify the status of the Postgres database connection using the **psql** command. You must sign in to the Linux shell from a remote support account to run this command; it is not accessible through

the administrator CLI. Run the following command after you install the Postgres database, but before you assign the database to an IM and Presence Service node.

Important For **psql** to run, you must first set an environment variable by entering:

```
$export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/xcp/lib
```

Enter:

```
$sudo -u xcpuser /usr/local/xcp/bin/psql -U db_user -h db_server db_name
```

For example:

```
$sudo -u xcpuser /usr/local/xcp/bin/psql -U postgres -h node1 tcmadb
```

- You can verify the status of the Oracle database connection by executing the following commands from the root:

```
export ORACLE_HOME=/usr/lib/oracle/client_1/
export PATH="$ORACLE_HOME/bin:$PATH"
export LD_LIBRARY_PATH="$ORACLE_HOME/lib:$LD_LIBRARY_PATH"
sqlplus username/password@dsn
```

  The *dsn* value can be obtained from the **$ORACLE_HOME/network/admin/tnsnames.ora** file.

- You can verify the status of the Microsoft SQL database connection by executing the following commands from the root:

```
$sudo -u xcpuser TDSVER=7.3 /usr/local/xcp/bin/tsql -H mssql_server_hostname -p portnumber
-U username -D databasename
```

- If you configure the message archiver (compliance) feature, and the Cisco XCP Message Archiver service fails to start, or you configure the persistent group chat feature and the Cisco Text Conference Manager service fails to start, check the External Database Troubleshooter section of the **System Configuration Troubleshooter** window.
  - If it shows that the status of the external database connection is not **OK**, verify that you provided the correct connection details and that there are no network issues between the IM and Presence Service node and the external database host.
  - If the status of the external database connection is **OK**, but the schema verification status is not, unassign the external database from the node, and reassign it again.
- Once the certificate is uploaded to the cup-xmpp-trust store, you must wait 15 minutes for the certificate to propagate to all the nodes of the IM and Presence Service cluster. If you do not wait, the SSL connection on nodes where the certificate has not propagated fails.
- If the certificate is missing or has been deleted from the cup-xmpp-trust store, an alarm 'XCPExternalDatabaseCertificateNotFound' is raised in the Cisco Unified Communications Manager `Real Time Monitoring Tool` (`RTMT`).

Note No alarm is raised if the external database type chosen is Microsoft SQL Server.