Intercluster Peer Configuration

Prerequisites for Intercluster Deployment

You configure an intercluster peer between the IM and Presence database publisher nodes in standalone IM and Presence Service clusters. No configuration is required on the IM and Presence Service subscriber nodes in a cluster for intercluster peer connections. Before you configure IM and Presence Service intercluster peers in your network, note the following:

- The intercluster peers must each integrate with a different Cisco Unified Communications Manager cluster.
- You must complete the required multinode configuration in both the home IM and Presence Service cluster, and in the remote IM and Presence Service cluster:
  - Configure the system topology and assign your users as required.
  - Activate the services on each IM and Presence Service node in the cluster.
- You must turn on the AXL interface on all local IM and Presence nodes, and on all remote IM and Presence nodes. IM and Presence Service creates, by default, an intercluster application user with AXL permissions. To configure an intercluster peer, you will require the username and password for the intercluster application user on the remote IM and Presence Service node.
- You must turn on the Sync Agent on the local IM and Presence database publisher node, and on the remote IM and Presence database publisher node. Allow the Sync Agent to complete the user sychronization from Cisco Unified Communications Manager before you configure the intercluster peers.

For sizing and performance recommendations for intercluster deployments, including information on determining a presence user profile, see the IM and Presence Service SRND.

Intercluster Peer Configuration

Configure Intercluster Peer

Perform this procedure on the database publisher node of the local IM and Presence Service cluster, and on the database publisher node of the remote IM and Presence Service cluster (with which you want your local cluster to form a peer relationship).

Before you begin

- Activate the AXL interface on all local IM and Presence Service nodes and confirm that the AXL interface is activated on all remote IM and Presence Service nodes.
- Confirm that the Sync Agent has completed the user synchronization from Cisco Unified Communications Manager on the local and remote cluster.
- Acquire the AXL username and password for the intercluster application user on the remote IM and Presence Service node.
- If you do not use DNS in your network, see topics related to IM and Presence Service default domain and node name values for intercluster deployments.
- Resolve any invalid or duplicate userIDs before proceeding. For more information, see topics related to end-user management and handling.

Note For the intercluster peer connection to work properly, the following ports must be left open if there is a firewall between the two clusters:

- 8443 (AXL)
- 7400 (XMPP)
- 5060 (SIP) Only if SIP federation is being used

Restriction

Cisco recommends that you use TCP as the intercluster trunk transport for all IM and Presence Service clusters.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Inter-Clustering**.

Step 2 Enter the IP address, FQDN, or hostname of the database publisher node of a remote IM and Presence Service cluster.

Step 3 Enter the username of the application user on the remote IM and Presence Service node that has AXL permissions.

Step 4 Enter the associated password of the application user on the remote IM and Presence Service node that has AXL permissions.

Step 5 Enter the preferred protocol for SIP communication.

Step 6 (Optional) Enter the External Phone Number Mask value. This is the E.164 mask to apply to Directory Numbers retrieved from the remote cluster.

Step 7 Click **Save**.

Step 8 Restart the Cisco XCP Router service on all nodes in the local cluster.

Step 9 Repeat this procedure on the database publisher node of the remote intercluster peer.

Tip If you configure the intercluster peer connection before the Sync Agent completes the user synchronization from Cisco Unified Communications Manager (on either the local or remote cluster), the status of the intercluster peer connection will display as Failed.

If you choose TLS as the intercluster transport protocol, IM and Presence Service attempts to automatically exchange certificates between intercluster peers to establish a secure TLS connection. IM and Presence Service indicates whether the certificate exchange is successful in the intercluster peer status section.

What to do next

Proceed to turn on the Intercluster Sync Agent.

Related Topics

Restart Cisco XCP Router Service
Node Name Value for Intercluster Deployments
IM and Presence Default Domain Value for Intercluster Deployments
Default Domain Value for Intercluster Deployments

Turn On Intercluster Sync Agent

By default, IM and Presence Service turns on the Intercluster Sync Agent parameter. Use this procedure to either verify that the Intercluster Sync Agent parameter is on, or to manually turn on this service.

The Intercluster Sync Agent uses the AXL/SOAP interface for the following:

- to retrieve user information for IM and Presence Service to determine if a user is a local user (on the local cluster), or a user on a remote IM and Presence Service cluster within the same domain.
- to notify remote IM and Presence Service clusters of changes to users local to the cluster.

Note You must turn on the Intercluster Sync Agent on all nodes in the IM and Presence Service cluster because in addition to synchronizing user information from the local IM and Presence database publisher node to the remote IM and Presence database publisher node, the Intercluster Sync Agent also handles security between all nodes in the clusters.

Procedure

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

Step 2 Choose the IM and Presence Service node from the Server menu.

Step 3 Choose **Cisco Intercluster Sync Agent**.

Step 4 Click **Start**.

What to do next

Proceed to verify the intercluster peer status.

Related Topics

Multinode Scalability Feature

Verify Intercluster Peer Status

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Inter-Clustering**.

Step 2 Choose the peer address from the search criteria menu.

Step 3 Click **Find**.

Step 4 Choose the peer address entry that you wish to view.

Step 5 In the **Intercluster Peer Status** window:

a) Verify that there are check marks beside each of the result entries for the intercluster peer.

b) Make sure that the Associated Users value equals the number of users on the remote cluster.

c) If you choose TLS as the intercluster transport protocol, the Certificate Status item displays the status of the TLS connection, and indicates if IM and Presence Service successfully exchanged security certificates between the clusters. If the certificate is out-of-sync, you need to manually update the tomcat trust certificate (as described in this module). For any other certificate exchange errors, check the Online Help for a recommended action.

Step 6 Choose **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**.

Step 7 Verify that there are check marks beside the status of each of the intercluster peer connection entries in the InterClustering Troubleshooter section.

Update Intercluster Sync Agent Tomcat Trust Certificates

If the tomcat certificate status for an intercluster peer is out-of-sync, you need to update the Tomcat trust certificate. In an intercluster deployment this error can occur if you reuse the existing Intercluster Peer Configuration to point to a new remote cluster. Specifically, in the existing Intercluster Peer Configuration window, you change the Peer Address value to point to a new remote cluster. This error can also occur in a fresh IM and Presence Service installation, or if you change the IM and Presence Service host or domain name, or if you regenerate the Tomcat certificate.

This procedure describes how to update the Tomcat trust certificate when the connection error occurs on the local cluster, and the corrupt Tomcat trust certificates are associated with the remote cluster.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Inter-Clustering.**

Step 2 Click **Force Sync** to synchronize certificates with the remote cluster.

Step 3 In the confirmation window that displays, choose **Also resync peer's Tomcat certificates**.

Step 4 Click **OK**.

Note If there are any certificates that have not synced automatically, go to the Intercluster Peer Configuration window and all certificates marked with an x are the missing certificates which you need to manually copy.

Delete Intercluster Peer Connections

Use this procedure if you want to remove an intercluster peer relationship.

Procedure

Step 1 Log in to the IM and Presence Service database publisher node.

Step 2 From Cisco Unified CM IM and Presence Administration, choose **Presence** > **Inter-Clustering**.

Step 3 Click **Find** and select the intercluster peer that you want to remove.

Step 4 Click **Delete**.

Step 5 Restart the **Cisco XCP Router**:

a) Log in to Unified IM and Presence Serviceability and choose **Tools** > **Control Center - Network Services**.
b) From the **Server** list, choose the database publisher node and click **Go**.
c) Under **IM and Presence Services**, select **Cisco XCP Router** and click **Restart**.

Step 6 Repeat these steps on the peer cluster.

Note If you are removing an intercluster peer from an intercluster network with multiple clusters, you must repeat this procedure for each peer cluster that remains in the intercluster network. This means that, on the cluster that is being removed, there will be as many cycles of **Cisco XCP Router** restarts as there are peer cluster connections that are being broken.