Configure Intercluster Peers

Intercluster Peers Overview

Intercluster peering provides the ability for users in one cluster to communicate and subscribe to the presence of users in a different cluster within the same domain. For large deployments you can use intercluster peering to connect your remote IM and Presence clusters.

Intercluster peering is configured on the database publisher node of both the local and the remote cluster.

For sizing and performance recommendations for intercluster deployments, see the chapter "Collaboration Instant Messaging and Presence" in the *Cisco Collaboration System Solution Reference Network Designs (SRND)* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/UCgoList.html#48016

Intercluster Peers Prerequisites

Before you configure IM and Presence Service intercluster peers in your network, note the following:

- Configure the system topology and assign your users as required for all clusters.
- 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
- For intercluster deployments, you must deploy a minimum OVA of 15,000 users. It is possible to have different clusters running different OVA sizes so long as all clusters are running at least the 15,000 user OVA.

Note Intercluster peering is not supported when the IM and Presence Service is deployed on a Cisco Business Edition 6000 server.

Intercluster Peers Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Check User Provisioning, on page 2	Verify that end users are correctly provisioned before you configure intercluster peers.
Step 2	Enable the Cisco AXL Web Service, on page 3	The Cisco AXL Web Service must be active on all local and remote IM and Presence nodes. Use this procedure to verify the service is running.
Step 3	Enable the Sync Agent, on page 3	Enable the Sync Agent on the database publisher node of each intercluster peer.
Step 4	Configure Intercluster Peers, on page 4	Complete this task on the database publisher node in each cluster to set up intercluster peers.
Step 5	Verify the Intercluster Sync Agent is On, on page 6	The Intercluster Sync Agent must be running on all nodes in the IM and Presence Service cluster. Use this procedure to verify that the Intercluster Sync Agent parameter is running.
Step 6	Verify Intercluster Peer Status, on page 6	Verify that the intercluster peer configuration works.
Step 7	Update Intercluster Sync Agent Tomcat Trust Certificates, on page 7	If the tomcat certificate status for an intercluster peer is out-of-sync, update the Tomcat trust certificate.
Step 8	Enable Auto Recovery for Intercluster Peer Periodic Syncing Failure, on page 7	Use this procedure to enable auto recovery for intercluster periodic syncing failure.
Step 9	Configure Intercluster Peer Sync Interval, on page 8	Use this procedure to set the time interval for intercluster peer syncing.
Step 10	Disable Certificate Sync for Intercluster Peer Periodic Sync, on page 9	Use this procedure to configure disable/enable of certificates sync as part of Intercluster periodic sync.

Check User Provisioning

Use this procedure to verify that end users are correctly provisioned before you configure intercluster peers.

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Diagnostics** > **System Troubleshooter**. The System Troubleshooter runs.

Step 2 In the **User Troubleshooter** section, verify that end users are correctly provisioned and that there are no duplicate or invalid users.

What to do next

Enable the Cisco AXL Web Service, on page 3

Enable the Cisco AXL Web Service

The Cisco AXL Web Service must be running on all local and remote IM and Presence cluster nodes. By default, this service is running. However, you can use this procedure to verify that the service is running.

Note When you enable the Cisco AXL Web Service, the system creates an intercluster application user with AXL permissions. You will need the username and password for the intercluster application user when you configure interlcuster peers on the remote IM and Presence Service node.

Procedure

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

Step 2 From the **Server** list, choose the node on which you want to reactivate services and click **Go**.

Step 3 In the **Database and Admin Services** area, check the **Status** of the **Cisco AXL Web Service**.

- If the service is **Started**, no action is required.
- If the service is **Not Running**, select the service and click **Restart**.

Step 4 Repeat this procedure on all cluster nodes in the local and remote clusters.

What to do next

Enable the Sync Agent, on page 3

Enable the Sync Agent

The Cisco Sync Agent must be running on the database publisher node of each intercluster peer.on the local and remote IM and Presence database publisher nodes.

Procedure

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

Step 2 From the **Server** drop-down list box, choose the IM and Presence database publisher node and click **Go**.

Step 3 Under **IM and Presence Services**, verify that the **Cisco Sync Agent** status is **Running**.

Step 4 If the service is not running, select the service and click **Restart**.

Step 5 Repeat this procedure in each cluster

What to do next

After the Cisco Sync Agent completes the user sync from Cisco Unified Communications Manager,Configure Intercluster Peers, on page 4

Configure Intercluster Peers

Use this procedure on the database publisher node for both the local and remote cluster to set up an intercluster peer relationship.

Before you begin

- Confirm that the Sync Agent has completed the user synchronization from Cisco Unified Communications Manager on the local and remote cluster. If you configure the intercluster peer connection before the Sync Agent completes the user sync, the status of the intercluster peer connection displays as **Failed**.
- Make sure that you have the AXL username and password for the intercluster application user on the remote IM and Presence Service node.

Procedure

Step 1 In Cisco Unified CM IM and Presence Administration, choose **Presence** > **Inter-Clustering**.

Step 2 Click **Add New**.

Step 3 In the **Peer Address** field, enter the node name of the remote cluster's database publisher node. This field may be an IP address, hostname or FQDN, but must match the actual node name that defines the server.

Note

- To verify the type of address the node name uses, log in to the Cisco Unified CM IM and Presence Administration on the remote cluster and choose **System** > **Presence Topology**. This window displays the node name and server details for each cluster node.
- Split-brain scenario may occur in a cluster that is part of multicluster environment. For example, there is a cluster A, and its multicluster peers are cluster B, C, D, and E. Nodes in cluster A must be able to reach DNS during split-brain scenario, because they have to communicate with other clusters B, C, D, and E in a multicluster environment during split-brain scenario.

  During split-brain scenario, If the nodes in cluster A cannot reach DNS then the IP addresses of A,B,C,D, and E cluster nodes should be set as node names, and NOT the hostnames and FQDNs.

  If the nodes in cluster A,B,C,D, and E are defined with FQDNs or hostnames, and they are not able to reach DNS during split-brain scenario, then service outages such as loss of IM Presence updates and loss of IM history occurs between clusters A and B,C,D,E.

Step 4 Enter the AXL credentials.

Step 5 Select the preferred **Protocol** for SIP communication.

Note Cisco recommends that you use **TCP** (the default setting) as the intercluster trunk transport for all IM and Presence Service clusters. You can change this setting if it suits your network configuration and security needs.

Step 6 Click **Save**.

Step 7 Check your notifications in the top right of the GUI header. If a notification advises you to restart the **Cisco XCP Router**, then do the following. Otherwise, you can skip this step:

a) From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.
b) From the **Server** drop-down list box, choose an IM and Presence node and click **Go**.
c) Select **Cisco XCP Router** and click **Restart**.
d) Repeat these steps on all cluster nodes

Step 8 Repeat this procedure on the database publisher node of each remote peer cluster.

Tip If you choose **TLS** as the intercluster transport protocol, the 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

Verify the Intercluster Sync Agent is On, on page 6

Restart the XCP Router Service

Restart the Cisco XCP Router service on all nodes in the local cluster, as well as all nodes in the remote cluster.

Before you begin

Configure Intercluster Peers, on page 4

Procedure

Step 1 From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.
Step 2 From the **Server** list, choose the node on which you want to reactivate services and click **Go**.
Step 3 In the **IM and Presence Services** area, select **Cisco XCP Router**.
Step 4 Click **Restart**.

What to do next

Verify the Intercluster Sync Agent is On, on page 6

Verify the Intercluster Sync Agent is On

The Intercluster Sync Agent network service synchronizes user information between intercluster peers. Use this procedure to confirm that the service is running on all cluster nodes in each intercluster peer.

Procedure

Step 1 From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.
Step 2 From the **Server** menu, choose an IM and Presence Service node and click **Go**.
Step 3 Confirm that the **Cisco Intercluster Sync Agent** displays a status of **Running**.
Step 4 If the service is not running, select the service and click **Start**.
Step 5 Repeat this procedure for all cluster nodes on each intercluster peer.

What to do next

Verify Intercluster Peer Status, on page 6

Verify Intercluster Peer Status

Use this procedure to confirm that your intercluster peer configurations are working properly.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Presence** > **Inter-Clustering**.
Step 2 Choose the peer address from the search criteria menu.
Step 3 Click **Find**.
Step 4 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 chose **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 5 Run the System Troubleshooter:

a) From Cisco Unified CM IM and Presence Administration, choose **Diagnostics** > **System Troubleshooter**.
b) In the **Inter-Clustering Troubleshooter** section, verify that there are check marks beside the status of each of the intercluster peer connection entries.

What to do next

Update Intercluster Sync Agent Tomcat Trust Certificates, on page 7

Update Intercluster Sync Agent Tomcat Trust Certificates

If a connection error appears occurs on the local cluster, and the corrupt Tomcat trust certificates are associated with the remote cluster, use this procedure to update the Tomcat trust certificate.

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

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **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. All certificates marked with an X are the missing certificates which you need to copy manually.

Enable Auto Recovery for Intercluster Peer Periodic Syncing Failure

Use this procedure to Enable this service parameter, if you want Cisco Intercluster Sync Agent to raise an “InterClusterSyncAgentPeerPeriodicSyncingFailure” alarm and to restart automatically, when Intercluster peer periodic sync is stuck for more than 2 hours.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **System** > **Service Parameters**.

Step 2 From the Server list, choose the IM and Presence node on which you want to set the "General Inter Cluster Sync Agent Parameters".

Step 3 From the **Service** list, choose **Cisco Intercluster Sync Agent (Active)**.

Step 4 Set the **Enable Auto Recovery for Inter-Cluster Peer Periodic Syncing Failure** service parameter to **Enabled**.

Step 5 Click **Save**.

Note If the "Enable Auto Recovery for Inter-cluster Peer Periodic Syncing Failure" service parameter is set to Enabled and if periodic sync is stuck for more than 2 hours then :

- ***InterClusterSyncAgentPeerPeriodicSyncingFailure*** Alarm will be generated.
- ***Cisco Intercluster Sync Agent*** service will be restarted automatically.

If "Enable Auto Recovery for Inter-cluster Peer Periodic Syncing Failure" is Disabled then :

- ***InterClusterSyncAgentPeerPeriodicSyncingFailure*** Alarm will be generated.
- ***Cisco Intercluster Sync Agent*** service will not be restarted automatically.

Configure Intercluster Peer Sync Interval

Use this procedure to set the time interval for intercluster peer syncing. The service parameter **Inter Cluster Peer Periodic Sync Interval (mins)** allows you to configure the time interval for dynamic ICSA periodic sync. The default setting for the intercluster peer sync interval is 30 minutes.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **System** > **Service Parameters**.

Step 2 From the Server list, choose the IM and Presence node on which you want to set the "General Inter Cluster Sync Agent Parameters".

Step 3 From the **Service** list, choose **Cisco Intercluster Sync Agent (Active)**.

Step 4 Set the **Inter Cluster Peer Periodic Sync Interval (mins)** service parameter to the desired interval. The range is 30 – 1444 minutes with a default of 30 minutes.

Step 5 Click **Save**.

Note The new setting takes effect following the next intercluster sync.

If the intercluster peer sync fails, the Cisco Intercluster Sync Agent service restarts following the completion of four sync periods. For example, if the parameter is set to 40 minutes, the service restarts after 160 minutes (4*40).

Disable Certificate Sync for Intercluster Peer Periodic Sync

Use this procedure to disable certificates sync as part of the intercluster sync process. The service parameter **Certificate Sync during Inter-Cluster Periodic Sync** allows the administrator to disable or enable certificates sync as part of the intercluster periodic sync. The default value of this service parameter is **Perform certificate sync**.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **System** > **Service Parameters**.

Step 2 From the Server list, choose the IM and Presence node on which you want to set the **General Inter Cluster Sync Agent Parameters**.

Step 3 From the **Service** list, choose **Cisco Intercluster Sync Agent (Active)**.

Step 4 Set the service parameter **Certificate Sync during Inter-Cluster Periodic Sync** to **Do not perform certificate sync**.

Step 5 Click **Save**.

Note If you encounter performance degradation or high CPU spikes in your deployment that is related to certificate sync during intercluster periodic sync, you can use this procedure to set the service parameter.

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 Repeat these steps on the peer cluster.

Note The IM and Presence Service is enhanced to prevent restart of XCP router on each node within the IM and Presence cluster after deleting an intercluster peer. This enhancement helps the administrator manage large-scale clusters effectively by significantly reducing the overhead caused by sequential restart of nodes while ensuring uninterrupted Jabber service.

Intercluster Peering Interactions and Restrictions

Feature	Interactions and Restrictions
Cisco Business Edition 6000	Intercluster peering is not supported when the IM and Presence Service is deployed on a Cisco Business Edition 6000 server.
Cluster Limit	With intercluster peering, you can deploy up to 30 IM and Presence Service clusters in the intercluster mesh, irrespective of whether those clusters are centralized or decentralized.
Intercluster Sync Agent resource shortage in multi cluster deployment	ICSA requires more resources in multi cluster deployment with large number of clusters. In case you face any issues with ICSA or SRM due to resource shortage. We recommend you to change the below mentioned Cisco SIP Proxy Service Parameters from default value of 20 to a new value of 10. • Maximum no. of processes • Maximum no. of spare processes • Maximum no. of processes Restart the SIP Proxy Service for the changes to take effect. Restart SRM and ICSA services.
Intercluster Sync Agent and DNS	Intercluster Sync Agent uses DNS to resolve all CUCM and IM&P servers listed in peer cluster's tomcat certificate (SAN entries). If the DNS resolution fails, Intercluster Sync Agent will not connect to the remote peer.