High Availability Deployment Configuration

- High Availability Deployments, page 1
- Turn On or Off High Availability for Subcluster, page 5
- Configure Advanced Service Parameters for Server Recovery Manager, page 7
- Perform Manual Failover to Backup Node, page 9
- Perform Manual Fallback to Primary Node, page 10
- Perform Manual Recovery of Subcluster, page 11

High Availability Deployments

High Availability Requirements

The IM and Presence Service supports High Availability at a subcluster level. Both nodes in the subcluster must be running the same version of IM and Presence Service software for High Availability to work.

High Availability Subcluster

IM and Presence Service supports High Availability in a subcluster meaning if a node in the subcluster fails, the Instant Message and Availability services from that node can failover to the second node in the subcluster.

You must manually turn on High Availability in a subcluster on the Cluster Topology interface on IM and Presence Service Administration interface. On the main Cluster Topology interface, the subcluster icon indicates that you have turned on High Availability on the subcluster.

A green tick beside the High Availability icon indicates that High Availability in the subcluster is running normally. A red "x" beside the High Availability icon indicates that the subcluster is in a failed state.

IM and Presence Service automatically detects failover in a subcluster by monitoring the heartbeat and monitoring the critical services on the peer node. When IM and Presence Service detects failover, it automatically moves all users to the backup node and supports automatic fallback to the primary node. From the Cisco Unified CM IM and Presence Administration interface, you can initiate a manual fallback to the primary node.
IM and Presence Service performs an automatic fallback when the backup activated node fails due to a critical service failure and the peer node is in the “Failed Over” state and supports the automatic recovery fallback.

To monitor and troubleshoot the status of the High Availability functionality on a subcluster, view the High Availability states that IM and Presence Service assigns to each node. If a failover occurs, on the node detail screen, IM and Presence Service marks the users that have failed over to the backup node.

**Related Topics**

- Node States, Causes and Recommended Actions

### Failover Impact to Clients and Services

During failover to the backup node, availability and instant messaging services are temporarily unavailable on client applications. After failover is complete, the availability and instant messaging services become available on the client again when the client signs back in. Similarly, if fallback occurs, availability and instant messaging services are temporarily unavailable on client applications until fallback completes and the client signs back in. Cisco Jabber signs users back in automatically.

The impact of failover on temporary ad hoc chat messages depends on the particular client application. On Cisco Jabber, any ad hoc chat windows that were open before failover should display again after the failover is complete. However, if all of the users in a chat room automatically exit the chat room as part of a failover or fallback process, or if the ad hoc chat room is hosted on a failed node, the ad hoc chat windows will not display again after failover and a message is displayed explaining that the chat room was deleted. On all clients, any persistent chat rooms that users create on the failed node cannot be accessed again until recovery. If Cisco Jabber is operating in softphone mode (the user is on a voice call) during failover, the voice call is not disconnected.

### Automatic Failover Detection

IM and Presence Service uses these methods to automatically detect if a node fails:

- **Peer Heartbeat** - In a subcluster, each node sends heartbeat intervals to the other node to check if the node is up and running. If a node detects a loss of heartbeat in the peer node, the node initiates a failover. You can configure the heartbeat interval and the heartbeat timeout from the Service Parameters page on Cisco Unified CM IM and Presence Administration interface.

- **Monitor Critical Services** - Each node monitors a list of critical services. If the node detects that any critical service is not running for a configurable outage period (ninety seconds is the default value), it instructs the peer node to initiate a failover. You can configure this critical service delay from the Service Parameters page on Cisco Unified CM IM and Presence Administration interface. These are the list of critical services that the node monitors:
  - Cisco DB (internal IDS database)
  - Cisco Presence Engine (if you activate this service)
  - Cisco XCP Router
Cisco Message Archiver (if you integrate IM and Presence Service with a third-party off-board database, and you activate this service)

Cisco SIP Proxy (if you configure SIP federation or you enable Partitioned Intradomain Federation and you activate this service)

Cisco XCP SIP Federation Connection Manager (if you configure SIP federation, or enable Partitioned Intradomain Federation, and you activate this service)

Cisco Presence Datastore

Cisco Route Datastore (if you configure SIP federation or you enable Partitioned Intradomain Federation and you activate this service)

You can view the critical services that IM and Presence Service monitors for failover on the node details screen on the Cluster Topology interface. The critical services that IM and Presence Service monitors are marked in the “Monitored” column in the services list.

**Note**

- IM and Presence Service only detects a failover if a critical service is not running for the duration of the outage period. It does not detect a failover in the case where one or more critical services are not running during the outage period, but not for the duration of the outage period, for example, a rolling outage. In this case, IM and Presence Service generates alarms indicating that services are starting and stopping, and you can perform a manual failover on IM and Presence Service.

- If you manually stop a critical service, and the service is stopped for longer than the permitted outage period, failover will occur.

Prior to Release 8.6, if IM and Presence Service detects the situation where both nodes in the subcluster think they own the same user, both nodes go into a failed state, and you need to perform a manual recovery from the Cluster Topology interface. In IM and Presence Service Release 9.0(1) and later, manual recovery is not required. When the network issue is resolved, auto-recovery occurs without administrator intervention.

If manual recovery is required for another reason, you may experience IDS replication delays.

To check the status of the IDS replication on a node either:

- Use this CLI command:
  
  ```bash
  utils dbreplication runtimestate
  ```

- Use the Cisco Unified IM and Presence Reporting Tool. The "IM and Presence Database Status" report displays a detailed status of the cluster.

**Related Topics**

Cisco Replication Watcher Service

**Automatic Fallback**

IM and Presence Service supports automatic fallback to the primary node after a failover. Automatic fallback is the process of moving users back to the primary node after a failover without manual intervention. You can enable automatic fallback with the Enable Automatic Fallback service parameter on the Cisco Unified CM IM and Presence Administration interface.
Automatic fallback occurs in the following scenarios:

- A critical service on Node A fails—A critical service (for example, the Presence Engine) fails on Node A. Automatic failover occurs and all users are moved to Node B. Node A is in a state called "Failed Over with Critical Services Not Running." When the critical service recovers, the node state changes to "Failed Over." When this occurs Node B tracks the health of Node A for 30 minutes. If no heartbeat is missed in this timeframe and the state of each node remains unchanged, automatic fallback occurs.

- Node A is rebooted—Automatic failover occurs and all users are moved to Node B. When Node A returns to a healthy state and remains in that state for 30 minutes automatic fallback will occur.

- Node A loses communications with Node B—Automatic failover occurs and all users are moved to Node B. When communications are re-established and remain unchanged for 30 minutes automatic fallback will occur.

If failover occurs for a reason other than one of the three scenarios listed here, you must recover the node manually. If you do not want to wait 30 minutes before the automatic fallback, you can perform a manual fallback to the primary node.

**Cisco Server Recovery Manager (SRM)**

The Cisco Server Recovery Manager (SRM) on IM and Presence Service manages the failover between nodes in a subcluster. The Cisco Server Recovery Manager manages all state changes in a node; state changes are either automatic or initiated by the administrator (manual).

After you turn on High Availability in a subcluster, the Cisco Server Recovery Manager on each node establishes heartbeat connections with the peer node, and begins to monitor the critical processes.

The SRM is responsible for the user move operations after it detects that failover has occurred. It is the SRM on the peer node, not on the failed node, that performs the user move operation. For example, if node A fails, the SRM on node B performs the user move operation. The SRM throttles the number of users moved to the peer node, it moves the users in batches or iterations. You can configure the number of users that the SRM moves per iteration (the default value is 25). On failover, the SRM will move users that are signed in first, and then move users that are not signed in. Note that if you initiate a fallback or if an automatic fallback occurs, users that are not signed in are moved first, and then users that are signed in.

If the SRM is not turned on, it does not monitor any critical processes, nor does it monitor the heartbeat connections with the peer node.

---

**Caution**  
Before you turn on High Availability in a subcluster, you must configure the SRM service parameters to properly reflect your deployment.

**Related Topics**

- High Availability Login Profiles
- Node State Definitions

**Manual Failover and Fallback**

From the Cluster Topology interface, you can perform the following procedures:
• Initiate a manual failover for a subcluster. When you initiate a manual failover, the Cisco Server Recovery Manager stops the critical services on the failed node, and moves all users to the backup node.

• Initiate a manual fallback from the Cluster Topology interface, where the Cisco Server Recovery Manager restarts critical services on the primary node and moves users back to the primary node.

• Perform a manual recovery for a subcluster (when both nodes in the subcluster are in a failed state). When you perform a manual recovery, IM and Presence Service restarts the Cisco Server Recovery Manager service on both nodes in the subcluster.

**High Availability and Intercluster Deployment Consideration**

When failover occurs, the Intercluster Sync Agent is responsible for communicating the user move information to other clusters. The Intercluster Sync Agent runs on both the publisher and subscriber nodes in a cluster. In an Active-Standby configuration, if the publisher node fails or the Intercluster Sync Agent on the publisher node fails, the Intercluster Sync Agent on the subscriber node becomes Active and resumes synchronization, meaning the other clusters will continue to receive the information that users have moved to a different node. Intercluster presence and IM continue to work. Users that have failed over will receive availability information for remote users. Remote users continue to receive availability information and IMs from users that have failed over, and all IMs they send to a failed over user are delivered. When the publisher node recovers, the publisher falls back to Active mode and the subscriber returns to Standby mode.

**Turn On or Off High Availability for Subcluster**

⚠️ **Caution**

Before you turn on High Availability in a subcluster, you must configure the SRM service parameters to properly reflect your deployment, see topics related to High Availability client login profiles.

You have to manually turn on High Availability in a subcluster; IM and Presence Service does not turn on High Availability in a subcluster by default. You can turn on High Availability in a subcluster when:

- there are two nodes in the subcluster, and
- both nodes have IP addresses that are resolvable addresses, and
- both nodes are running IM and Presence Service Release 9.0 or higher.

You can either assign users to the nodes in the subcluster before or after you turn on High Availability for the subcluster.

**Before You Begin**

- Configure the subclusters and nodes in your network, and assign nodes to the subclusters.
- Make sure critical services are running on both nodes in the subcluster before you turn on high-availability in a subcluster. If one or more critical services are not running on a node, when you turn on High Availability, that node will failover to the backup node. When one or more critical services are not running on one node in a subcluster, but all critical services are running on the second node, the subcluster will go into a failed state after you turn on High Availability.

**Restriction**
You can only turn on High Availability in a subcluster when there are two nodes assigned to that subcluster. The High Availability checkbox does not display when there are no nodes, or one node, assigned to the subcluster.

**Procedure**

**Step 1** Cisco Unified CM IM and Presence Administration > System > Cluster Topology.

**Step 2** Select the edit link on the appropriate subcluster.

**Step 3** Check **Enable High Availability**.

*Note* To turn off High Availability for the subcluster, uncheck **Enable High Availability**.

**Step 4** Select **Save**.

IM and Presence Service displays the following information about High Availability for the subcluster:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitored Node</td>
<td>The node in the subcluster that IM and Presence is monitoring for failover detection.</td>
</tr>
<tr>
<td>Node State</td>
<td>The state of the node.</td>
</tr>
<tr>
<td>Node Reason</td>
<td>The reason for the node state.</td>
</tr>
<tr>
<td>Node Action</td>
<td>The action you can take to change the state of the node:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fallback</strong> - This option is displayed for nodes that are in Idle or Failed Over states. Select to manually initiate a fallback to this node.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Failover</strong> - This option is displayed for nodes that are in Normal state. Select to manually initiate a failover to this node.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Recovery</strong> - This option is displayed if both nodes in the subcluster are in a failed state. Select to manually initiate a recovery of the subcluster where IM and Presence Service restarts the SRM service on both nodes.</td>
</tr>
</tbody>
</table>

**Troubleshooting Tips**

• When you turn on High Availability in a subcluster, IM and Presence Service restarts the Cisco Service Recovery Manager service and it begins to monitor for failover detection. To verify this service is running, select **Cisco Unified IM and Presence Serviceability > Tools > Control Center - Network Services**.

• You can turn off High Availability in a subcluster, so the two nodes in the subcluster act as standalone nodes. You can only turn off High Availability when the nodes in the subcluster are not in a transition state (Failing Over, Falling Back). If you turn off High Availability in a subcluster when either node is in a failed over scenario (Failed Over, Failed), users that IM and Presence Service fails over to the backup node are homed to the backup node. IM and Presence Service will not move these users back to the primary node, they remain on the backup node.
The System Troubleshooter indicates if there are any two node subclusters without High Availability turned on. Select Cisco Unified CM IM and Presence Administration > Diagnostics > System Troubleshooter.

**Related Topics**
- High Availability Login Profiles
- Node State Definitions
- Node States, Causes and Recommended Actions

## Configure Advanced Service Parameters for Server Recovery Manager

The following table describes the advanced service parameters you can configure for the Server Recovery Manager.

**Table 1: Advanced Server Recover Manager Service Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Port</td>
<td>This parameter specifies the port that Cisco Server Recovery Manager uses to communicate with its peer.</td>
<td>If you modify this parameter, IM and Presence Service restarts the Cisco Server Recovery Manager on all nodes in the cluster.</td>
</tr>
<tr>
<td>Admin RPC Port</td>
<td>This parameter specifies the port that Cisco Server Recovery Manager uses to provide admin RPC requests.</td>
<td>If you modify this parameter, IM and Presence Service restarts the Cisco Server Recovery Manager on all nodes in the cluster.</td>
</tr>
<tr>
<td>Critical Service Down Delay</td>
<td>This parameter determines the duration a critical service can be down before IM and Presence Service initiates an automatic failover.</td>
<td>If you change this value, this affects how long a critical service can be down before IM and Presence Service initiates an automatic failover.</td>
</tr>
<tr>
<td>Enable Automatic Fallback</td>
<td>This parameter turns automatic fallback on or off on IM and Presence Service.</td>
<td>This parameter is off by default.</td>
</tr>
<tr>
<td>Initialization Keep Alive</td>
<td>This parameter specifies the duration that the heartbeat is lost with the peer node (SRM) when the peer SRM restarts and is in the initialization state.</td>
<td>We recommend that you configure this value to at least twice the value of the Keep Alive (Heartbeat) Timeout in order to avoid unnecessary failovers.</td>
</tr>
</tbody>
</table>
### Additional Information

**Description**
This parameter specifies the duration that the heartbeat is lost with the peer node (SRM) before IM and Presence Service initiates an automatic failover.

**Additional Information**
We recommend that you configure this value to at least twice the value of KeepAliveInterval value. If this value is too close to the KeepAliveInterval value, this can cause a failover to occur.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep Alive (Heartbeat) Timeout</td>
<td>This parameter specifies the interval between keep alive (heartbeat) messages sent to the peer node.</td>
<td>N/A</td>
</tr>
<tr>
<td>Keep Alive (Heart Beat) Interval</td>
<td>This parameter specifies the number of users that IM and Presence Service moves for each iteration when it performs a failover or a fallback. There is a delay of one second between each iteration.</td>
<td>Increasing this value will shorten the failover time at the expense of CPU. Lowering the value will lengthen failover time, but have less impact on the CPU. <strong>Caution</strong> Before you configure the Users Moved Per Iteration parameter value, refer to the High Availability client login profiles.</td>
</tr>
<tr>
<td>Users Moved Per Iteration</td>
<td>This parameter specifies the minimum number of seconds which Cisco Jabber will wait before attempting to re-login to this IM and Presence Service node. This waiting time occurs due to the failure of a node or a critical service on a node. <strong>Note</strong> This parameter is per node.</td>
<td><strong>Caution</strong> Refer to the High Availability client login profiles for guidelines on defining the client re-login lower and upper limits.</td>
</tr>
<tr>
<td>Client Re-Login Lower Limit</td>
<td>This parameter specifies the maximum number of seconds which Cisco Jabber will wait before attempting to re-login to this IM and Presence Service node. This waiting time occurs due to the failure of a node or a critical service on a node. <strong>Note</strong> This parameter is per node.</td>
<td><strong>Caution</strong> Refer to the High Availability client login profiles for guidelines on defining the client re-login lower and upper limits.</td>
</tr>
</tbody>
</table>

### Procedure

1. **Step 1**  
   Cisco Unified CM IM and Presence Administration > System > Service Parameters.
2. **Step 2**  
   Select an IM and Presence Service node from the Server menu.
3. **Step 3**  
   Select Cisco Server Recovery Manager from the Service menu.
4. **Step 4**  
   Configure the service parameters.
Step 5  Select Save.

Related Topics
High Availability Login Profiles

Perform Manual Failover to Backup Node

You can perform a manual failover to the backup node in the subcluster using the Cluster Topology interface. When you initiate a manual failover, the Cisco Server Recovery Manager stops the critical services on that node, and moves all users to the backup node.

The Cisco Server Recovery Manager stops the following critical services on the node:

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Router (this causes all XCP processes to stop)
- Cisco Client Profile Agent

The Cisco Server Recovery Manager then move all users to the backup node

Restriction
You can only initiate a failover for a node that is in "Normal" state.

Before You Begin
Make sure that these services are running on the Failing Over node:

- Cisco XCP Connection Manager service
- Cisco XCP Router
- Cisco Presence Engine

Procedure

Step 1  Cisco Unified CM IM and Presence Administration > System > Cluster Topology.
Step 2  Select the edit link on the appropriate subcluster.
Step 3  Select Failover in the Node Action column.
Step 4  Select Ok to confirm the failover operation.
Step 5  To verify the failover operation is complete and successful:

a)  When the failover operation is in progress, the primary node should be in the “Failing Over” state, and the backup node should be in the “Taking Over” state. When the failover operation is complete, check that the backup node is in the state "Running in Backup Mode", and the primary node is in "Idle" state. If the failover is unsuccessful, and the nodes are in a failed state.

b)  Check that the users have failed over to the backup node:
• On the subcluster details screen, check that all users are now assigned to the backup node, and no users are assigned to the primary node.

• On the node details screen, the “Failed Over” column indicates the users that have failed over to the backup node.

---

**Related Topics**

Node States, Causes and Recommended Actions

---

**Perform Manual Fallback to Primary Node**

You can perform a manual fallback to the primary node in the Cluster Topology interface. When you initiate a manual fallback, the Cisco Server Recovery Manager restarts any critical services that are not already running on the primary node, and moves the failed over users back to the primary node.

When you manually initiate a fallback, the Cisco Server Recovery Manager restarts the following services on the primary node (if they are not already running):

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Router
- Any XCP services that were activated
- Cisco Client Profile Agent

The Cisco Server Recovery Manager then moves all failed over users back to the primary node.

**Restriction**

You can only initiate fallback for a node that is in 'Idle' or 'Failed Over' state.

**Procedure**

**Step 1**  
Cisco Unified CM IM and Presence Administration &gt; System &gt; Cluster Topology.

**Step 2**  
Select the edit link on the appropriate subcluster.

**Step 3**  
Select **Fallback** in the Node Action column.

**Step 4**  
Select **Ok** to confirm the fallback operation.

**Step 5**  
To verify the fallback operation is complete and successful:

a) When fallback operation is in progress, the primary node should be in the “Taking Back” state, and the backup node should be in the “Falling Back” state. When the fallback operation is complete, check that both nodes are in 'Normal' state. If the fallback is unsuccessful, and the nodes are in a failed state.

b) Check that the users have fallen back to the primary node.

• On the subcluster details screen, check that all users are now assigned to the primary node, and no users are assigned to the backup node.
• On the node details screen, the “Failed Over” column should be empty.

---

Related Topics

Node States, Causes and Recommended Actions

Perform Manual Recovery of Subcluster

When you perform a manual recovery of a subcluster, IM and Presence Service restarts the Cisco Server Recovery Manager service on both nodes in the subcluster.

Restriction

You can only initiate a recovery for a subcluster if both nodes are in a failed state.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Cisco Unified CM IM and Presence Administration &gt; System &gt; Cluster Topology.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select the edit link on the appropriate subcluster.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Recovery in the Node Action column.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Verify the status of the subcluster after you perform the manual recovery.</td>
</tr>
</tbody>
</table>

Troubleshooting Tips

In prior releases, if two nodes in the subcluster think that they own the same user, both nodes will go into a failed state, and you had to perform a manual recovery from the Cluster Topology interface. In this release manual recovery is not required. When the network issue is resolved, auto-recovery occurs without administrator intervention.

If manual recovery is required for another reason, you may experience IDS replication delays. You can check the status of the IDS replication on a node using this CLI command:

Utils dbreplication runtimestate

---

Related Topics

Node States, Causes and Recommended Actions
Perform Manual Recovery of Subcluster