Post-Change Tasks and Verification

Post-Change Task List for Cisco Unified Communications Manager Nodes

The following table lists the tasks to perform after you have changed the IP address or hostname of the Unified Communications Manager nodes in your cluster.

Perform the tasks that apply to your deployment in the order in which they are presented in the task list. For details about system health checks or generating ITL certificates, see the related topics.

⚠ **Caution** If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Table 1: Post-Change Task List for Unified Communications Manager Nodes

Item	Task
System health checks	
1	Ensure that all servers in the cluster are up and available, and check for any active ServerDown alerts. **Note** ServerDown alerts in the Syslog are normal during the change process, but should not appear in the log after the change is done.

Item	Task
2	Check the database replication status of all Unified Communications Manager nodes in the cluster to ensure that all servers are replicating database changes successfully. **Note** Verify the hostname changes of the publisher and subscriber nodes in the cluster. If the hostname changes are not replicated, you need to restart the 'A Cisco DB' service of all the other nodes in the cluster.
3	Check network connectivity and DNS server configuration on the node that was changed using the CLI command `utils diagnose module validate_network`.
4	In Cisco Unified Reporting, generate the Unified CM Database Status report. Look for any errors or warnings in this report.
5	In Cisco Unified Reporting, generate the Unified CM Cluster Overview report. Look for any errors or warnings in this report.
Security enabled cluster tasks	
6	For security-enabled clusters (Cluster Security Mode 1 - Mixed), update the CTL file and then restart all nodes in the cluster before you perform the system health checks and other post-change tasks. For detailed instructions on updating and managing the CTL file, including adding a new TFTP server to an existing CTL file, see the Security Guide for Cisco Unified Communications Manager.
7	If you enabled cluster security using Certificate Trust List (CTL) files and USB eTokens, you must regenerate the Initial Trust List (ITL) file and the certificates in the ITL if you changed the IP address or hostname for Release 8.0 or later nodes. Skip this step if you have not enabled cluster security using Certificate Trust List (CTL) files and USB eTokens.
Post-change tasks	
8	Run a manual DRS backup and ensure that all nodes and active services back up successfully. For more information, see the Administration Guide for Cisco Unified Communications Manager. **Note** You must run a manual DRS backup after you change the IP address of a node, because you cannot restore a node with a DRS file that contains a different IP address or hostname. The post-change DRS file will include the new IP address or hostname.
9	Update all relevant IP phone URL parameters.
10	Update all relevant IP phone services using Cisco Unified Communications Manager Administration.
11	Update Unified RTMT custom alerts and saved profiles.
12	If you are using the integrated DHCP server that runs on Unified Communications Manager, update the DHCP server.

Item	Task
13	Check and make any required configuration changes to other associated Cisco Unified Communications components, such as Cisco Unity Connection and Cisco Unified MeetingPlace Express. **Note** Consult the documentation for your product to determine how to make any required configuration changes.
14	Reset the phone after you change the DNS IP address for the phone to reflect the updated information. Resetting the phone clears the phone cache.
15	When you change the hostname or remove the node from the cluster, you need to remove the node from the intercluster, wait until syncing of the nodes and configure the node again in the cluster.

Related Topics

Check System Health

Perform Post-Change Tasks for Cisco Unified Communications Manager Nodes, on page 5

Initial Trust List and Certificate Regeneration, on page 7

Post-Change Task List for IM and Presence Service Nodes

The following table lists the tasks to perform after you have changed the IP address, hostname, domain name, or the node name of the IM and Presence Service nodes in your cluster.

Perform the tasks in the order in which they are presented in the task list.

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Table 2: Post-Change Task List for IM and Presence Service Nodes

Item	Task
System health checks	
1	Verify that changes to the hostname or IP address are updated on the Cisco Unified Communications Manager server.
2	Check network connectivity and DNS server configuration on the node that was changed. **Note** If you changed the IP address to a different subnet, ensure that your network adapter is now connected to the correct VLAN. Also, if the IM and Presence Service nodes belong to different subnets after the IP address change, ensure that the Routing Communication Type field of the Cisco XCP Router service parameter is set to **Router to Router**. Otherwise, the Routing Communication Type field should be set to **Multicast DNS**.
3	Verify that the changes to the IP address, hostname, or both are fully implemented in the network.

Item	Task
4	If you changed the hostname, verify that the hostname change has been fully implemented in the network. **Note** Verify the hostname changes of the publisher and subscriber nodes in the cluster. If the hostname changes are not replicated, you need to restart the 'A Cisco DB' service of all the other nodes in the cluster.
5	Verify that database replication has been successfully established. All nodes should show a status of **2** and be **Connected**. If replication is not set up, see topics related to troubleshooting database replication.
Post-change tasks	
6	If you disabled OpenAM SSO prior to performing a procedure, you can enable it now. For information about how to enable OpenAM SSO, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.
7	Ensure that the cup, cup-xmpp and Tomcat certificates contain the new hostname.
8	If the IP address for a node has changed, update Unified RTMT custom alerts and saved profiles.
9	Check and make any required configuration changes to other associated Cisco Unified Communications components, for example, SIP trunks on Cisco Unified Communications Manager.
10	Start all network services that are listed under the CUP Services group. You must start the CUP Services network services in the prescribed order. **Note** You do not need to complete this step if you are changing the IP address, hostname, or both the IP address and hostname. Network services are automatically started for these name changes. However, if some services do not automatically start after the change, complete this step to ensure that all network services are started.
11	Start all feature services. The order in which you start feature services is not important. **Note** You do not need to complete this step if you are changing the IP address, hostname, or both the IP address and hostname. Feature services are automatically started for these name changes. However, if some services do not automatically start after the change, complete this step to ensure that all feature services are started.
12	If you disabled HA during the pre-change setup, confirm that your Cisco Jabber sessions have been recreated before you re-enable High Availability. Otherwise, Jabber clients whose sessions are created will be unable to connect. Run the `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI command on all cluster nodes. The number of active sessions should match the number of users that you recorded when you disabled high availability. If it takes more than 30 minutes for your sessions to start, you may have a larger system issue. Once you are sure that your Jabber sessions are created, re-enable High Availability in all presence redundancy groups.
13	Verify that IM and Presence Service is functioning properly after the changes.

Item	Task
14	Run a manual Disaster Recovery System backup after you change the IP address or hostname of a node.

Related Topics

Check System Health

Perform Post-Change Tasks for IM and Presence Service Nodes, on page 8

Perform Post-Change Tasks for Cisco Unified Communications Manager Nodes

Perform all post-change tasks to ensure that your changes are properly implemented in your deployment.

Perform the tasks in the order in which they are presented in the task list.

⚠ **Caution** If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Before you begin

- Perform all applicable system health checks to verify the changes that were made to your deployment.
- Perform the security enabled cluster tasks if cluster security is enabled for your deployment.

Procedure

Step 1 Run a manual DRS backup and ensure that all nodes and active services back up successfully.

For more information, see the *Administration Guide for Cisco Unified Communications Manager* .

Note You must run a manual DRS backup after you change the IP address of a node, because you cannot restore a node with a DRS file that contains a different IP address or hostname. The post-change DRS file will include the new IP address or hostname.

Step 2 Update all relevant IP phone URL parameters.

Step 3 Update all relevant IP phone services using Cisco Unified Communications Manager Administration. Choose **System** > **Enterprise Parameters**.

Step 4 Update Unified RTMT custom alerts and saved profiles.

- Unified RTMT custom alerts that are derived from performance counters include the hard-coded server IP address. You must delete and reconfigure these custom alerts.
- Unified RTMT saved profiles that have performance counters include the hard-coded server IP address. You must delete and re-add these counters and then save the profile to update it to the new IP address.

Step 5 If you are using the integrated DHCP server that runs on Cisco Unified Communications Manager, update the DHCP server.

Step 6 Check and make any required configuration changes to other associated Cisco Unified Communications components.

The following is a partial list of some of the components to check:

- Cisco Unity
- Cisco Unity Connection
- CiscoUnity Express
- SIP/H.323 trunks
- IOS Gatekeepers
- Cisco Unified MeetingPlace
- Cisco Unified MeetingPlace Express
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- DHCP Scopes for IP phones
- SFTP servers that are used for Cisco Unified Communications Manager trace collection for CDR export, or as a DRS backup destination
- IOS hardware resources (conference bridge, media termination point, transcoder, RSVP agent) that register with Cisco Unified Communications Manager
- IPVC video MCUs that register or integrate with Cisco Unified Communications Manager
- Cisco Emergency Responder
- Cisco Unified Application Environment
- Cisco Unified Presence
- Cisco Unified Personal Communicator
- Associated routers and gateways

Note Consult the documentation for your product to determine how to make any required configuration changes.

Security enabled cluster tasks for Cisco Unified Communications Manager nodes

Initial Trust List and Certificate Regeneration

If you change the IP address or the hostname of a server in a Cisco Unified Communications Manager Release 8.0 or later cluster, the Initial Trust List (ITL) file and the certificates in the ITL are regenerated. The regenerated files do not match the files stored on the phones.

Note If you enable cluster security using Certificate Trust List (CTL) files and USB eTokens, it is not necessary to perform the steps in the following procedure because trust is maintained by the eTokens and the eTokens are not changed.

If cluster security is not enabled, perform the steps in the Single-server cluster or Multi-server cluster procedures to reset the phones.

Regenerate certificates and ITL for single-server cluster phones

If you change the IP address or the hostname of the server in a Cisco Unified Communications Manager Release 8.0 or later single-server cluster and you are using ITL files, perform the following steps to reset the phones.

Enable rollback prior to changing the IP address or hostname of the server.

Procedure

Step 1 Ensure that all phones are online and registered so that they can process the updated ITLs. For phones that are not online when this procedure is performed, the ITL must be deleted manually.

Step 2 Set the Prepare Cluster for Rollback to pre-8.0 enterprise parameter to True. All phones automatically reset and download an ITL file that contains empty Trust Verification Services (TVS) and TFTP certificate sections.

Step 3 On the phone, select **Settings** > **Security** > **Trust List** > **ITL File** to verify that the TVS and TFTP certificate sections of the ITL file are empty.

Step 4 Change the IP address or hostname of the server and let the phones configured for rollback register to the cluster.

Step 5 After all the phones have successfully registered to the cluster, set the enterprise parameter Prepare Cluster for Rollback to pre-8.0 to **False**.

What to do next

If you use CTL files or tokens, re-run the CTL client after you change the IP address or hostname of the server, or after you change the DNS domain name.

Certificate and ITL Regeneration for Multi-Server Cluster Phones

In a multi-server cluster, the phones should have primary and secondary TVS servers to validate the regenerated ITL file and certificates. If a phone can not contact the primary TVS server (due to recent configuration changes), it will fall back to the secondary server. The TVS servers are identified by the CM Group assigned to the phone.

In a multi-server cluster, ensure that you change the IP address or hostname on only one server at a time. If you use CTL files or tokens, re-run the CTL client or the CLI command set **utils ctl** after you change the IP address or hostname of the server, or after you change the DNS domain name.

Perform Post-Change Tasks for IM and Presence Service Nodes

Perform all post-change tasks to ensure that your changes are properly implemented in your deployment.

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Before you begin

Perform all the applicable verification system health checks to verify the changes that were made to your deployment.

Procedure

Step 1 If you disabled OpenAM single sign-on (SSO), you can enable it now. For more information about OpenAM SSO, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Step 2 If you changed the hostname, you must ensure that the cup, cup-xmpp and Tomcat certificates contain the new hostname.

a) From the Cisco Unified OS Administration GUI, select **Security** > **Certificate Management**.
b) Verify that the names of the trust certificates contain the new hostname.
c) If the certificates do not contain the new hostname, regenerate the certificates.

   For more information, see the *Administration Guide for Cisco Unified Communications Manager* .

Step 3 If the IP address for a node has changed, update Cisco Unified Real-Time Monitoring Tool (RTMT) custom alerts and saved profiles:

- RTMT custom alerts that are derived from performance counters include the hard-coded server address. You must delete and reconfigure these custom alerts.
- RTMT saved profiles that have performance counters include the hard-coded server address. You must delete and re-add these counters and then save the profile to update it to the new address.

Step 4 Check and make any required configuration changes to other associated Cisco Unified Communications components, for example, SIP trunks on Cisco Unified Communications Manager.

Step 5 Start all network services that are listed under the CUP Services group using Cisco Unified Serviceability, select **Tools** > **Control Center - Network Services**.

Tip You do not need to complete this step if you are changing the IP address, hostname, or both the IP address and hostname. Network services are automatically started for these name changes. However, if some services do not automatically start after the change, complete this step to ensure that all network services are started.

You must start the CUP Services network services in the following order:

a. Cisco IM and Presence Data Monitor
b. Cisco Server Recovery Manager
c. Cisco Route Datastore
d. Cisco Login Datastore
e. Cisco SIP Registration Datastore
f. Cisco Presence Datastore
g. Cisco XCP Config Manager
h. Cisco XCP Router
i. Cisco OAM Agent
j. Cisco Client Profile Agent
k. Cisco Intercluster Sync Agent
l. Cisco Config Agent

Step 6 Start all feature services using Cisco Unified Serviceability, select **Tools** > **Control Center - Feature Services**. The order in which you start feature services is not important.

Tip You do not need to complete this step if you are changing the IP address, hostname, or both the IP address and hostname. Feature services are automatically started for these name changes. However, if some services do not automatically start after the change, complete this step to ensure that all feature services are started.

Step 7 Confirm that your Cisco Jabber sessions have been recreated before you re-enable High Availability. Otherwise, Jabber clients whose sessions are created will be unable to connect.

Run the `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI command on all cluster nodes. The number of active sessions should match the number of users that you recorded when you disabled high availability. If it takes more than 30 minutes for your sessions to start, you may have a larger system issue.

Step 8 Enable High Availability (HA) on all presence redundancy groups if you disabled HA during the pre-change setup.

Step 9 Verify that IM and Presence Service is functioning properly after the changes.

a) From the Cisco Unified Serviceability GUI, select **System** > **Presence Topology**.

- If HA is enabled, verify that all HA nodes are in the Normal state.
- Verify that all services are started.

b) Run the System Troubleshooter from the Cisco Unified CM IM and Presence Administration GUI and ensure that there are no failed tests. Select **Diagnostics** > **System Troubleshooter**.

Step 10 You must run a manual Disaster Recovery System backup after you change the IP address or hostname of a node, because you cannot restore a node with a DRS file that contains a different IP address or hostname. The post-change DRS file will include the new IP address or hostname.

For more information, see the *Administration Guide for Cisco Unified Communications Manager* .