Post Change Tasks And Verification

Post-Change Tasks Cisco Unified Communications Manager 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.

Procedure

Step 1 If you have DNS configured anywhere on the Cisco Unified Communications Manager servers, ensure that a forward and reverse lookup zone has been configured and that the DNS is reachable and working.

Step 2 Check for any active ServerDown alerts to ensure that all servers in the cluster are up and available. Use either the Cisco Unified Real-Time Monitoring Tool (RTMT) or the command line interface (CLI) on the first node.

a) To check using Unified RTMT, access Alert Central and check for ServerDown alerts.

b) To check using the CLI on the first node, enter the following CLI command and inspect the application event log:

```
file search activelog syslog/CiscoSyslog ServerDown
```

Step 3 Check the database replication status on all nodes in the cluster to ensure that all servers are replicating database changes successfully.

For IM and Presence Service, check the database replication status on the database publisher node using the CLI if you have more than one node in your deployment.

Use either Unified RTMT or the CLI. All nodes should show a status of **2**.

a) To check by using RTMT, access the Database Summary and inspect the replication status.
b) To check by using the CLI, enter **utils dbreplication runtimestate**.

   For example output, see topics related to example database replication output. For detailed procedures and troubleshooting, see topics related to verifying database replication and troubleshooting database replication.

Step 4 Enter the CLI command **utils diagnose** as shown in the following example to check network connectivity and DNS server configuration.

Example:

```
admin: utils diagnose module validate_network
Log file: /var/log/active/platform/log/diag1.log

Starting diagnostic test(s)
===========================
test - validate_network    : Passed

Diagnostics Completed
admin:
```

If you are performing the pre-change system health checks, you are done; otherwise, continue to perform the post-change verification steps.

Step 5 Verify that the new hostname or IP address appears on the Cisco Unified Communications Manager server list. In Cisco Unified Communications Manager Administration, select **System** > **Server**.

Note Perform this step only as part of the post-change tasks.

Step 6 Verify that changes to the IP address, hostname, or both are fully implemented in the network. Enter the CLI command **show network cluster** on each node in the cluster.

Note Perform this step only as part of the post-change tasks.

The output should contain the new IP address or hostname of the node.

Example:

```
admin:show network cluster
10.63.70.125 hippo2.burren.pst hippo2 Subscriber cups DBPub authenticated
10.63.70.48 aligator.burren.pst aligator Publisher callmanager DBPub
authenticated using TCP since Wed May 29 17:44:48 2013
```

Step 7 Verify that changes to the hostname are fully implemented in the network. Enter the CLI command **utils network host** <***new_hostname***> on each node in the cluster.

Note Perform this step only as part of the post-change tasks.

The output should confirm that the new hostname resolves locally and externally to the IP address.

Example:

```
admin:utils network host hippo2
Local Resolution:
hippo2.burren.pst resolves locally to 10.63.70.125

External Resolution:
hippo2.burren.pst has address 10.63.70.125
```

tasks.

Step 8 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 more information, see the Certificate and ITL Regeneration for Multi-Server Cluster Phones, on page 5 section.

Step 9 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.

Step 10 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 11 Update all relevant IP phone URL parameters.

Step 12 Update all relevant IP phone services using Cisco Unified Communications Manager Administration. Choose **System** > **Enterprise Parameters**.

Step 13 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 14 If you are using the integrated DHCP server that runs on Cisco Unified Communications Manager, update the DHCP server.

Step 15 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.

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.

Procedure

Step 1 Verify that changes to the hostname or IP address are updated on the Cisco Unified Communications Manager server.

Step 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.

Step 3 Verify that the changes to the IP address, hostname, or both are fully implemented in the network.

Step 4 If you changed the hostname, verify that the hostname change has been fully implemented in the network.

Step 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.

Step 6 If you disabled SAML single sign-on (SSO), you can enable it now. For more information about SAML SSO, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Step 7 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 8 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 9 Check and make any required configuration changes to other associated Cisco Unified Communications components, for example, SIP trunks on Cisco Unified Communications Manager.

Step 10 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 11 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 12 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 13 Enable High Availability (HA) on all presence redundancy groups if you disabled HA during the pre-change setup.

Step 14 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 15 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* .