Pre-Change Tasks and System Health Checks

Pre-Change Task List for Cisco Unified Communications Manager Nodes

The following table lists the tasks to perform before you proceed to change the IP address and hostname for Cisco Unified Communications Manager nodes. You must perform these procedures during a scheduled maintenance window. Perform all system health checks before you perform the pre-change setup tasks.

For details about any of the tasks that are listed, see topics related to performing system health checks on nodes and pre-change setup.

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: Pre-Change Task List for Cisco Unified Communications Manager Nodes

Item	Task
System health checks	
1	If you have DNS configured anywhere on the Cisco Unified Communications Manager servers, ensure that forward and reverse records (for example, A record and PTR record) are configured and that the DNS is reachable and working.
2	Ensure that all servers in the cluster are up and available, and check for any active ServerDown alerts.
3	Check the database replication status of all Cisco Unified Communications Manager nodes in the cluster to ensure that all servers are replicating database changes successfully.

Item	Task
4	Check network connectivity and DNS server configuration.
Pre-change setup tasks	
5	Use Cisco Unified Communications Manager Administration to compile a list of all nodes in the cluster. Retain this information for use later.
6	Run a manual Disaster Recovery System backup and ensure that all nodes and active services are backed up successfully. For more information, see the *Administration Guide for Cisco Unified Communications Manager* .
7	For security-enabled clusters (Cluster Security Mode 1 - Mixed), update the Certificate Trust List (CTL) file. For detailed instructions on updating and managing the CTL file, including adding a new TFTP server to an existing CTL file, see the *Cisco Unified Communications Manager Security Guide*. All IP phones that support security always download the CTL file, which includes the IP address of the TFTP servers with which the phones are allowed to communicate. If you change the IP address of one or more TFTP servers, you must first add the new IP addresses to the CTL file so that the phones can communicate with their TFTP server. **Caution** To avoid unnecessary delays, you must update the CTL file with the new IP address of your TFTP servers before you change the IP address of the TFTP servers. If you do not perform this step, you will have to update all secure IP phones manually. **Note** Note: This is not applicable when the CallManager certificate is a Multi-SAN certificate.

Related Topics

Check System Health, on page 4
Perform Pre-Change Setup Tasks for Cisco Unified Communications Manager Nodes, on page 6

Pre-Change Task List for IM and Presence Service Nodes

The following table lists the tasks to perform before you proceed to change the IP address, hostname, domain name, or the node name for IM and Presence Service nodes. You must perform these procedures during a scheduled maintenance window. Perform all system health checks before you perform the pre-change setup tasks.

For details about any of the tasks that are listed, see topics related to performing system health checks on nodes and pre-change setup.

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: Pre-Change Task List for IM and Presence Service Nodes

Item	Task
System health checks	
1	Check the database replication status to ensure that all nodes are replicating database changes successfully if you have more than one IM and Presence Service node in your deployment.
2	Check network connectivity and DNS server configuration.
Pre-change setup tasks	
3	Run a manual Disaster Recovery System backup and ensure that all nodes are backed up successfully. For more information, see the *Administration Guide for Cisco Unified Communications Manager* .
4	Disable High Availability (HA) on all presence redundancy groups. For more information about how to disable HA, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.
5	If you are changing the hostname, disable single sign-on (SSO). For more information about SSO, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.
6	Compile a list of all services that are currently activated on the node.
7	Stop all feature services for the node.
8	Stop IM and Presence Service network services for the node in the specified order. For a detailed list of the network services to stop and the order in which to stop them, see the procedure to perform pre-change setup tasks for IM and Presence Service nodes.
9	For IM and Presence Service node name and domain name changes, verify that the Cisco AXL Web Service is started on the Cisco Unified Communications Manager publisher node.
10	For IM and Presence Service node name and domain name changes, verify on the IM and Presence database publisher node that the Cisco Sync Agent service has started and that synchronization is complete using either the Cisco Unified Serviceability GUI or the System Dashboard on Cisco Unified CM IM and Presence Administration.

Related Topics

Check System Health, on page 4
Perform Pre-Change Setup Tasks for IM and Presence Service Nodes, on page 7

System Health Checks

Check System Health

Perform the applicable system health checks on the nodes in your deployment as part of the pre-change setup and as part of the post-change tasks that you must perform after you have changed any network identifiers.

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.

Some of the checks in this procedure are required only for post-change verification. See the post-change task list for a complete list of the system health checks to perform.

Note If you are performing system health checks as part of the pre-change setup, you can skip the following steps which are only required when you are performing the post-change tasks:

- Verification that the new hostname or IP address appears on the Cisco Unified Communications Manager server list.
- Verification that changes to the IP address, hostname, or both are fully implemented in the network.
- Verification that changes to the hostname are fully implemented in the network.

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 (Post-change step) 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 (Post-change step) 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 (Post-change step) 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
```

Related Topics

- Example Database Replication CLI Output
- Reset Database Replication
- Repair Database Replication
- Troubleshoot Cluster Authentication
- Troubleshoot Database Replication
- Troubleshoot Network
- Verify Database Replication

Pre-Change Setup

Perform all pre-change setup tasks to ensure that your system is prepared for a successful IP address, hostname, domain, or node name change. You must perform these tasks during a scheduled maintenance window.

You should perform the system health checks on your deployment before performing the pre-change setup.

Perform Pre-Change Setup Tasks for Cisco Unified Communications Manager Nodes

Perform the following pre-change setup tasks before you change the IP address or hostname. You must perform these tasks during a scheduled maintenance window. See the pre-change task list for more information.

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 the system health checks on your deployment.

Procedure

Step 1 From Cisco Unified Communications Manager Administration on the first node, select **System** > **Server** and click **Find**. A list of all servers in the cluster displays. Retain this list of servers for future reference.

Ensure that you save an inventory of both the hostname and IP address of each node in your cluster.

Step 2 Run a manual Disaster Recovery System backup and ensure that all nodes and active services are backed up successfully.

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

Step 3 For security-enabled clusters (Cluster Security Mode 1 - Mixed), update the Certificate Trust List (CTL) file.

For detailed instructions on updating and managing the CTL file, including adding a new TFTP server to an existing CTL file, see the *Cisco Unified Communications Manager Security Guide*.

Note All IP phones that support security always download the CTL file, which includes the IP address of the TFTP servers with which the phones are allowed to communicate. If you change the IP address of one or more TFTP servers, you must first add the new IP addresses to the CTL file so that the phones can communicate with their TFTP server.

Caution To avoid unnecessary delays, you must update the CTL file with the new IP address of your TFTP servers before you change the IP address of the TFTP servers. If you do not perform this step, you will have to update all secure IP phones manually.

Perform Pre-Change Setup Tasks for IM and Presence Service Nodes

Perform the applicable pre-change setup tasks to ensure that your system is prepared for a successful IP address, hostname, domain, or node name change. You must perform these tasks during a scheduled maintenance window. See the pre-change task list for more information.

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.

Note You do not need to perform the steps to verify that the Cisco AXL Web service and the IM and Presence Cisco Sync Agent services are started unless you are changing the domain name or the node name. See the pre-change task list for a complete list of the tasks to perform.

Before you begin

Perform the system health checks on your deployment.

Procedure

Step 1 Run a manual Disaster Recovery System backup and ensure that all nodes and active services are backed up successfully.

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

Step 2 Disable High Availability (HA) on all presence redundancy groups. For information on Presence Redundancy Groups configuration, see the "Configure Presence Redundancy Groups" chapter in the *System Configuration Guide for Cisco Unified Communications Manager*.

Note
- Before you disable HA, take a record of the number of users in each node and subcluster. You can find this information in the **System** > **Presence Topology** window of Cisco Unified CM IM and Presence Administration.
- After you disable HA, wait at least 2 minutes for the settings to sync across the cluster before completing any further changes.

Step 3 If you are changing the hostname, disable OpenAM single sign-on (SSO). For more information about OpenAM SSO, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Step 4 Compile a list of all services that are currently activated. Retain these lists for future reference.

a) To view the list of activated network services using Cisco Unified Serviceability, select **Tools** > **Control Center - Network Services**.

b) To view the list of activated feature services using Cisco Unified Serviceability, select **Tools** > **Control Center - Feature Services**.

Step 5 Stop all feature services using Cisco Unified Serviceability, select **Tools** > **Control Center - Feature Services**. The order in which you stop 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 stopped for these name changes.

Step 6 Stop the following network services that are listed under the IM and Presence Service services group using Cisco Unified Serviceability when you select **Tools** > **Control Center - Network Services**.

You must stop these IM and Presence Service network services in the following order:

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

Step 7 Verify that the Cisco AXL Web Service is started on the Cisco Unified Communications Manager publisher node using Cisco Unified Serviceability, **Tools** > **Control Center - Feature Services**.

Note Perform this step only if you are changing the domain name or node name.

Step 8 Verify that the IM and Presence Cisco Sync Agent service has started and that synchronization is complete.

Note Perform this step only if you are changing the domain name or node name.

a) To verify using Cisco Unified Serviceability, perform the following steps:

1. Select **Tools** > **Control Center - Network Services**.
2. Select the IM and Presence database publisher node.

3. Select **IM and Presence Service Services**.
4. Verify that the Cisco Sync Agent service has started.
5. From the Cisco Unified CM IM and Presence Administration GUI, select **Diagnostics** > **System Dashboard** > **Sync Status**.
6. Verify that synchronization is complete and that no errors display in the synchronization status area.

b) To verify using the Cisco Unified CM IM and Presence Administration GUI on the IM and Presence database publisher node, select **Diagnostics** > **System Dashboard**.