Manage the Server

Manage the Server Overview

This chapter describes how to manage the properties of the Cisco Unified Communications Manager node, view the Presence Server status and configure a host name for the Unified Communications Manager server.

Server Deletion

This section describes how to delete a server from the Cisco Unified Communications Manager database and how to add a deleted server back to the Cisco Unified Communications Manager cluster.

In Cisco Unified Communications Manager Administration, you cannot delete the first node of the cluster, but you can delete subsequent nodes. Before you delete a subsequent node in the Find and List Servers window, Cisco UnifiedCM Administration displays the following message: “You are about to permanently delete one or more servers. This action cannot be undone. Continue?”. If you click OK, the server gets deleted from the Cisco UnifiedCM database and is not available for use.

Tip When you attempt to delete a server from the Server Configuration window, a message that is similar to the one in the preceding paragraph displays. If you click OK, the server gets deleted from the Cisco UnifiedCM database and is not available for use.

Before you delete a server, consider the following information:

- Cisco Unified Communications Manager Administration does not allow you to delete the first node in the cluster, but you can delete any subsequent node.

- Cisco recommends that you do not delete any node that has Cisco Unified Communications Manager running on it, especially if the node has devices, such as phones, registered with it.
- Although dependency records exist for the subsequent nodes, the records do not prevent you from deleting the node.
- If any call park numbers are configured for Cisco Unified Communications Manager on the node that is being deleted, the deletion fails. Before you can delete the node, you must delete the call park numbers in Cisco Unified Communications Manager Administration.
- If a configuration field in Cisco Unified Communications Manager Administration contains the IP address or host name for a server that you plan to delete, update the configuration before you delete the server. If you do not perform this task, features that rely on the configuration may not work after you delete the server; for example, if you enter the IP address or host name for a service parameter, enterprise parameter, service URL, directory URL, IP phone service, and so on, update this configuration before you delete the server.
- If an application GUI, for example, Cisco Unity, Cisco Unity Connection, and so on, contains the IP address or host name for the server that you plan to delete, update the configuration in the corresponding GUIs before you delete the server. If you do not perform this task, features that rely on the configuration may not work after you delete the server.
- The system may automatically delete some devices, such as MOH servers, when you delete a server.
- Before you delete a node, Cisco recommends that you deactivate the services that are active on the subsequent node. Performing this task ensures that the services work after you delete the node.
- Changes to the server configuration do not take effect until you restart Cisco Unified Communications Manager. For information on restarting the Cisco CallManager service, see the *Cisco Unified Serviceability Administration Guide*.
- To ensure that database files get updated correctly, you must reboot the cluster after you delete a server, Presence, or application server.
- After you delete the node, access Cisco Unified Reporting to verify that Cisco Unified Communications Manager removed the node from the cluster. In addition, access Cisco Unified Reporting, RTMT, or the CLI to verify that database replication is occurring between existing nodes; if necessary, repair database replication between the nodes by using the CLI.

Note When a subscriber node is removed from a cluster, its certificates still exist in publisher and other nodes. Admin has to manually remove:

- the certificate of the subscriber node removed from the trust-store of the individual cluster members.
- the certificates of each of the other cluster members from the trust-store of the removed subscriber node.

Delete Unified Communications Manager Node from Cluster

Use this procedure to delete a Cisco Unified Communications Manager node from the cluster.

Procedure

Step 1 From Cisco Unified CM Administration choose **System** > **Server**.

Step 2 Click **Find** and select the node you want to delete.

Step 3 Click **Delete**.

Step 4 Click **OK** when a warning dialog box indicates that this action cannot be undone.

Step 5 Shut down the host VM for the node you have unassigned.

Delete IM and Presence Node From Cluster

Follow this procedure if you need to safely remove an IM and Presence Service node from its presence redundancy group and cluster.

Caution Removing a node will cause a service interruption to users on the remaining node(s) in the presence redundancy group. This procedure should only be performed during a maintenance window.

Procedure

Step 1 On the **Cisco Unified CM Administration > System > Presence Redundancy Groups** page, disable High Availability if it is enabled.

Step 2 On the **Cisco Unified CM Administration > User Management > Assign Presence Users** page, unassign or move all the users off the node that you want to remove.

Step 3 To remove the node from its presence redundancy group, choose **Not-Selected** from the Presence Server drop down list on the presence redundancy group's **Presence Redundancy Group Configuration** page. Select **OK** when a warning dialog box indicates that services in the presence redundancy group will be restarted as a result of unassigning the node.

Note You cannot delete the publisher node directly from a presence redundancy group. To delete a publisher node, first unassign users from the publisher node and delete the presence redundancy group completely.

However, you can add the deleted IM and Presence node back into the cluster. For more information on how to add the deleted nodes, see Add Deleted Server Back in to Cluster, on page 4. In this scenario, the **DefaultCUPSubcluster** is created automatically when the deleted publisher node is added back to the server in the **System > Server** screen in the Cisco Unified CM Administration console.

Step 4 In Cisco Unified CM Administration, delete the unassigned node from the **System** > **Server**. Click **OK** when a warning dialog box indicates that this action cannot be undone.

Step 5 Shut down the host VM or server for the node you have unassigned.

Step 6 Restart the **Cisco XCP Router** on all nodes.

Add Deleted Server Back in to Cluster

If you delete a subsequent node (subscriber) from Cisco Unified Communications Manager Administration and you want to add it back to the cluster, perform the following procedure.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, add the server by choosing **System** > **Server**.

Step 2 After you add the subsequent node to Cisco Unified Communications Manager Administration, perform an installation on the server by using the disk that Cisco provided in the software kit for your version.

Tip Make sure that the version that you install matches the version that runs on the publisher node. If the version that is running on the publisher does not match your installation file, choose the Upgrade During Install option during the installation process. For details, see the *Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service*.

Step 3 After you install Cisco UnifiedCM, configure the subsequent node, as described in the installation documentation that supports your version of Cisco UnifiedCM.

Step 4 Access the Cisco Unified Reporting, RTMT, or the CLI to verify that database replication is occurring between existing nodes; if necessary, repair database replication between the nodes.

Add Node to Cluster Before Install

Use Cisco Unified Communications Manager Administration to add a new node to a cluster before installing the node. The server type you select when adding the node must match the server type you install.

You must configure a new node on the first node using Cisco Unified Communications Manager Administration before you install the new node. To install a node on a cluster, see the *Cisco Unified Communications Manager Installation Guide*.

For Cisco Unified Communications Manager Video/Voice servers, the first server you add during an initial installation of the Cisco Unified Communications Manager software is designated the publisher node. All subsequent server installations or additions are designated as subscriber nodes. The first Cisco Unified Communications Manager IM and Presence node you add to the cluster is designated the IM and Presence Service database publisher node.

Note You cannot use Cisco Unified Communications Manager Administration to change the server type after the server has been added. You must delete the existing server instance, and then add the new server again and choose the correct server type setting.

Procedure

Step 1 Select **System** > **Server**.

The **Find and List Servers** window displays.

Step 2 Click **Add New**.

The **Server Configuration - Add a Server** window displays.

Step 3 From the **Server Type** drop-down list box, choose the server type that you want to add, and then click **Next**.

- CUCM Video/Voice
- CUCM IM and Presence

Step 4 In the **Server Configuration** window, enter the appropriate server settings.

For server configuration field descriptions, see Server Settings.

Step 5 Click **Save**.

View Presence Server Status

Use Cisco Unified Communications Manager Administration to view the status of critical services and self-diagnostic test results for the IM and Presence Service node.

Procedure

Step 1 Select **System** > **Server**.

The **Find and List Servers** window appears.

Step 2 Select the server search parameters, and then click **Find**.

Matching records appear.

Step 3 Select the IM and Presence server that is listed in the **Find and List Servers** window.

The **Server Configuration** window appears.

Step 4 Click on the Presence Server Status link in the IM and Presence Server Information section of the **Server Configuration** window.

The **Node Details** window for the server appears.

Configure Ports

Use this procedure to change the port settings used for connections such as SCCP device registration, SIP device registration, and MGCP gateway connections.

Note Normally, you need not change the default port settings. Use this procedure only if you really want to change the defaults.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **System** > **Cisco Unified CM**.
The **Find and List Cisco Unified CMs** window appears.

Step 2 Enter the appropriate search criteria and click **Find**.
All matching Cisco Unified Communications Managers are displayed.

Step 3 Select the **Cisco Unified CM** that you want to view.
The **Cisco Unified CM Configuration** window appears.

Step 4 Navigate to the **Cisco Unified Communications Manager TCP Port Settings for this Server** section.

Step 5 Configure the port settings for the Cisco Unified Communications Manager.

See Port Settings, on page 6 information about the fields and their configuration options.

Step 6 Click **Save**.

Step 7 Click **Apply Config**.

Step 8 Click **OK**.

Port Settings

Field	Description
Ethernet Phone Port	The system uses this TCP port to communicate with the Cisco Unified IP Phones (SCCP only) on the network. • Accept the default port value of 2000 unless this port is already in use on your system. Choosing 2000 identifies this port as non-secure. • Ensure all port entries are unique. • Valid port numbers range from 1024 to 49151.
MGCP Listen Port	The system uses this TCP port to detect messages from its associated MGCP gateway. • Accept the default port of 2427 unless this port is already in use on your system. • Ensure all port entries are unique. • Valid port numbers range from 1024 to 49151.

Field	Description
MGCP Keep-alive Port	The system uses this TCP port to exchange keepalive messages with its associated MGCP gateway. • Accept the default port of 2428 unless this port is already in use on your system. • Ensure all port entries are unique. • Valid port numbers range from 1024 to 49151.
SIP Phone Port	This field specifies the port number that Unified Communications Manager uses to listen for SIP line registrations over TCP and UDP.
SIP Phone Secure Port	This field specifies the port number that the system uses to listen for SIP line registrations over TLS.
SIP Phone OAuth Port	This field specifies the port number that Cisco Unified Communications Manager uses to listen for SIP line registrations from Jabber On-Premise devices over TLS (Transport Layer Security). The default value is 5090. Range is 1024 to 49151.
SIP Mobile and Remote Access OAuth Port	This field specifies the port number that Cisco Unified Communications Manager uses to listen for SIP line registrations from Jabber over Expressway through MTLS (Mutual Transport Layer Security). The default value is 5091. Range is 1024 to 49151.

Hostname Configuration

The following table lists the locations where you can configure a host name for the Unified Communications Manager server, the allowed number of characters for the host name, and the recommended first and last characters for the host name. Be aware that, if you do not configure the host name correctly, some components in Unified Communications Manager, such as the operating system, database, installation, and so on, may not work as expected.

Table 1: Host Name Configuration in Cisco Unified Communications Manager

Host Name Location	Allowed Configuration	Allowed Number of Characters	Recommended First Character for Host Name	Recommended Last Character for Host Name
Host Name/ IP Address field **System** > **Server** in Cisco Unified Communications Manager Administration	You can add or change the host name for a server in the cluster.	2-63	alphabetic	alphanumeric
Hostname field Cisco Unified Communications Manager installation wizard	You can add the host name for a server in the cluster.	1-63	alphabetic	alphanumeric

Host Name Location	Allowed Configuration	Allowed Number of Characters	Recommended First Character for Host Name	Recommended Last Character for Host Name
Hostname field **Settings** > **IP** > **Ethernet** in Cisco Unified Communications Operating System	You can change, not add, the host name for a server in the cluster.	1-63	alphabetic	alphanumeric
set network hostname hostname Command Line Interface	You can change, not add, the host name for a server in the cluster.	1-63	alphabetic	alphanumeric

Tip The host name must follow the rules for ARPANET host names. Between the first and last character of the host name, you can enter alphanumeric characters and hyphens.

Before you configure the host name in any location, review the following information:

- The Host Name/IP Address field in the Server Configuration window, which supports device-to-server, application-to-server, and server-to-server communication, allows you to enter an IPv4 address in dotted decimal format or a host name.

  After you install the Unified Communications Manager publisher node, the host name for the publisher automatically displays in this field. Before you install a Unified Communications Manager subscriber node, enter either the IP address or the host name for the subscriber node in this field on the Unified Communications Manager publisher node.

  In this field, configure a host name only if Unified Communications Manager can access the DNS server to resolve host names to IP addresses; make sure that you configure the Cisco Unified Communications Manager name and address information on the DNS server.

Tip In addition to configuring Unified Communications Manager information on the DNS server, you enter DNS information during the Cisco Unified Communications Manager installation.

- During the installation of the Unified Communications Manager publisher node, you enter the host name, which is mandatory, and IP address of the publisher node to configure network information; that is, if you want to use static networking.

  During the installation of a Unified Communications Manager subscriber node, you enter the hostname and IP address of the Unified Communications Manager publisher node, so that Unified Communications Manager can verify network connectivity and publisher-subscriber validation. Additionally, you must enter the host name and the IP address for the subscriber node. When the Unified Communications Manager installation prompts you for the host name of the subscriber server, enter the value that displays in the Server Configuration window in Cisco Unified Communications Manager Administration; that is, if you configured a host name for the subscriber server in the Host Name/IP Address field.

kerneldump Utility

The kerneldump utility allows you to collect crash dump logs locally on the affected machine without requiring a secondary server.

In a Unified Communications Manager cluster, you only need to ensure the kerneldump utility is enabled on the server before you can collect the crash dump information.

Note Cisco recommends that you verify the kerneldump utility is enabled after you install Unified Communications Manager to allow for more efficient troubleshooting. If you have not already done so, enable the kerneldump utility before you upgrade the Unified Communications Manager from supported appliance releases.

Important Enabling or disabling the kerneldump utility will require a reboot of the node. Do not execute the enable command unless you are within a window where a reboot would be acceptable.

The *command line interface* (CLI) for the *Cisco Unified Communications Operating System* can be used to enable, disable, or check the status of the kerneldump utility.

Use the following procedure to enable the kernel dump utility:

Working with Files That Are Collected by the Utility

To view the crash information from the kerneldump utility, use the *Cisco Unified Real-Time Monitoring Tool* or the *Command Line Interface* (CLI). To collect the kerneldump logs by using the *Cisco Unified Real-Time Monitoring Tool*, choose the Collect Files option from Trace & Log Central. From the Select System Services/Applications tab, choose the Kerneldump logs check box. For more information on collecting files using *Cisco Unified Real-Time Monitoring Tool*, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

To use the CLI to collect the kerneldump logs, use the "file" CLI commands on the files in the crash directory. These are found under the "activelog" partition. The log filenames begin with the IP address of the kerneldump client and end with the date that the file is created. For more information on the file commands, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Enable the Kerneldump Utility

Use this procedure to enable the kerneldump utility. In the event of a kernel crash, the utility provides a mechanism for collecting and dumping the crash. You can configure the utility to dump logs to the local server or to an external server.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Complete either of the following:

- To dump kernel crashes on the local server, run the `utils os kerneldump enable` CLI command.

- To dump kernel crashes to an external server, run the `utils os kerneldump ssh enable <ip_address>` CLI command with the IP address of the external server.

Step 3 Reboot the server.

Example

Note If you need to disable the kerneldump utility, you can run the `utils os kernelcrash disable` CLI command to disable the local server for core dumps and the `utils os kerneldump ssh disable <ip_address>` CLI command to disable the utility on the external server.

What to do next

Configure an email alert in the Real-Time Monitoring Tool to be advised of core dumps. For details, see Enable Email Alert for Core Dump, on page 10

Refer to the *Troubleshooting Guide for Cisco Unified Communications Manager* for more information on the kerneldump utility and troubleshooting.

Enable Email Alert for Core Dump

Use this procedure to configure the Real-Time Monitoring Tool to email the administrator whenever a core dump occurs.

Procedure

Step 1 Select **System** > **Tools** > **Alert** > **Alert Central**.

Step 2 Right-click **CoreDumpFileFound** alert and select **Set Alert Properties**.

Step 3 Follow the wizard prompts to set your preferred criteria:

a) In the **Alert Properties: Email Notification** popup, make sure that **Enable Email** is checked and click **Configure** to set the default alert action, which will be to email an administrator.

b) Follow the prompts and **Add** a Recipient email address. When this alert is triggered, the default action is to email this address.

c) Click **Save**.

Step 4 Set the default Email server:

a) Select **System** > **Tools** > **Alert** > **Config Email Server**.

b) Enter the e-mail server and port information to send email alerts.

c) (Optional) Check the **Enable TLS mode** check box for enabling encrypted communication channels to the SMTP server.

d) (Optional) Check the **Enable Authentication mode** check box to require authentication of the email address of the recipient.

Note The **Username** and **Password** fields are accessible only if the **Enable Authentication mode** check box is enabled.

e) Enter a user name in the **Username** field.
f) Enter a password in the **Password** field.
g) Enter the **Send User Id**.
h) Click **OK**.