Replace a Single Server or Cluster for Cisco Unified Communications Manager, Release 10.0(1)

First Published: December 03, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-29577-01

© 2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Replace a Single Server or Cluster v

Related documentation v

Obtain support vi

CHAPTER 1

Before you begin 1

System configuration information 4

Account names and passwords record 4

Record network configuration settings 5

Record SMTP settings 7

Record the hostname and timezone 7

Verify DNS registration 7

Determine registration counts 8

Record critical services 8

Locate system errors 9

Record trace log job details 9

Record CDR management configuration 10

Record system configuration counts 10

Record firmware information 11

Record system version 12

CHAPTER 2

Replace single server or cluster 13

Replace publisher node 14

Replace subscriber or dedicated TFTP server 15

Upgrade vSphere ESXi 16

Migrate from single to multi-vDisk virtual machine 16

Change virtual machine configuration specifications 17

CHAPTER 3 Complete replacement 19

Create backup 19

Supported features and components 19

Configure features for backup 20

Configure storage location 21

Start backup 22

Check backup status 22

Obtain license file 23

Verify NTP status 23

Install software on publisher server 23

Install software on subscriber server 26

Upload license file 29

Restore backup file 30

View restore status 31

Complete replacement 32

Upgrade server hardware 33

Memory recommendations 33

Upgrade hard drives 34

Adjust logging 35

Replace a Single Server or Cluster

This document describes how to replace a single server or an entire cluster for Cisco Unified Communications Manager. Replacement means that you replace the server hardware while preserving the server configuration. The replacement server operates identically to the old server.

Caution Because this process is designed to work as a server replacement, you need to do it in the live environment. Cisco does not recommend doing this process on a "dead net" because a duplication of the entire network environment is required, which is highly risky.

- Related documentation, page v
- Obtain support, page vi

Related documentation

For additional installation-related information, refer to the following documents:

- *Upgrading Cisco Unified Communications Manager*

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html
- *Installing Cisco Unified Communications Manager*

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html
- *Cisco Unified Communications Operating System Administration Guide*

  http://preview.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

For further information about related Cisco IP telephony applications and products, refer to the *Cisco Unified Communications Manager Documentation Guide*:

http://cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html.

The following table lists URLs for software and additional documentation.

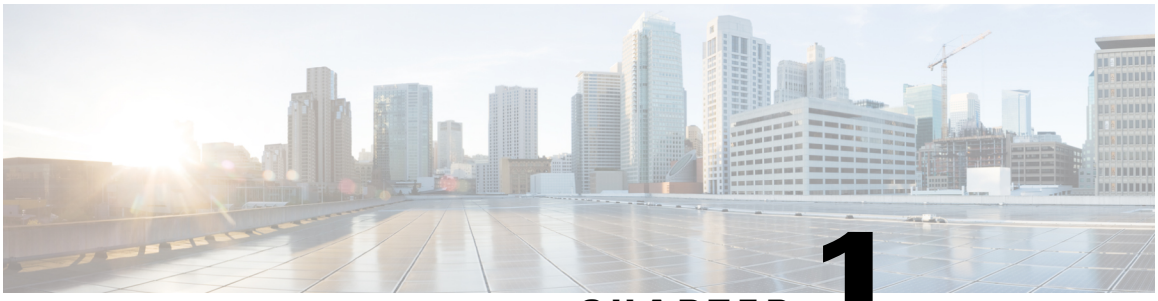
Table 1: Quick Reference for URLs

Related Information and Software	URL
Cisco MCS data sheets	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html
Software-only servers (IBM, HP, Compaq, Aquarius)	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html
Cisco Unified Communications Manager service releases	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

Obtain support

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html



CHAPTER 1

Before you begin

This section describes that tasks that you should perform before you begin the server or cluster replacement.

Procedure

Step 1 Verify the integrity of the new server hardware by running any manufacturer-provided utilities.

Step 2 Make sure that the new servers are listed as supported hardware and sized appropriately to support the load of cluster.
Refer to the following documentation for information about the capacity of server models:

- Release notes for your product release
- http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html

Make sure to account for any growth that has occurred since initial system configuration.

Step 3 Verify that links between servers meet the delay requirements and that you have enough bandwidth to support database replication.
For more information, refer to *Cisco Unified Communications SRND Based on Cisco Unified Communications Manager*.

Step 4 Record all system passwords and account IDs.
See the Account names and passwords record, on page 4.

You must enter identical passwords when configuring the replacement server. You cannot retrieve these passwords from the server.

Step 5 Make sure that you have a copy of all custom ring files, phone backgrounds, and music on hold sources.
Consider this actions as precautionary because the restore is designed to restore these items.

Step 6 Obtain and store COP files for any locales that are installed on the server.
You need to reinstall locales after doing the replacement.

Step 7 Do not change computer names or IP addresses, or add more nodes to the cluster.

Step 8 Verify the integrity of your software downloads and DVDs.
Perform the following tasks:

- Check the MD5 checksum of downloaded software against the published value to verify that it downloaded properly.
- Verify that the DVD is readable by a DVD drive.

Step 9 If your firewall is not in the routing path, disable the firewall between nodes, if possible. Also, increase the firewall timeout settings until after you complete the installation.
It is not always sufficient to temporarily allow network traffic in and out of the nodes (for example, setting the firewall rule for these nodes to IP any/any). The firewall might still close necessary network sessions between nodes due to timeouts.

Step 10 Perform any system tests that you intend to perform after the replacement before the replacement also, to verify that the tests pass before you do the replacement.
Document these tests, so you can perform them identically after doing the replacement.

Step 11 If you use DNS, verify that all servers that are to be replaced are configured in DNS properly. All nodes in the cluster must either use DNS or not use it.
See the Verify DNS registration, on page 7.

Step 12 Do not run Network Address Translation (NAT) or Port Address Translation (PAT) between Cisco Unified Communications Manager nodes.

Step 13 Record all the registration information by using the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT).
See the Determine registration counts, on page 8.

You cannot perform this task if your old server is not working.

Step 14 Record all the critical services and their activation status by using the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT).
See the Record critical services, on page 8.

You cannot perform this task if your old server is not working.

Step 15 Using the Syslog viewer in the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT), locate any events that have a severity of Error or higher.
Perform this task to ensure that no system-affecting errors exist on your system.

See the Locate system errors, on page 9.

You cannot perform this task if your old server is not working.

Step 16 Record the details of all Trace and Log Central jobs.
See the Record trace log job details, on page 9.

You cannot perform this task if your old server is not working.

Step 17 Record CDR Management configuration and destinations, if applicable.
See the Record CDR management configuration, on page 10.

You cannot perform this task if your old server is not working.

Step 18 From Cisco Unified Communications Manager Administration, determine the number of specific items that are configured on the server.
See the Record system configuration counts, on page 10.

You cannot perform this task if your old server is not working.

Step 19 From Cisco Unified Communications Manager Administration, record all the phone loads and device types that display on the Firmware Load Information window.
See the Record firmware information, on page 11.

If you have custom device types that do not ship with Cisco Unified Communications Manager, make sure that you have the appropriate COP files. You need to reinstall the devices types after performing the replacement.

You cannot perform this task if your old server is not working.

Step 20 Record all network configuration settings and other configuration settings that are described in the sections that are referenced in the Important Notes column for each server to be replaced.
See the following sections:

- Record network configuration settings, on page 5.
- Record SMTP settings, on page 7
- Record the hostname and timezone, on page 7

You cannot perform this task if your old server is not working.

Step 21 Compare the system version on each node in your cluster by using Cisco Unified Communications Manager Administration. Verify that you have DVDs with that version.
See the Record system version, on page 12.

If you have a service release, you need media for the base release and the service release.

Step 22 If your cluster is running in secure mode, make sure that you have USB eToken devices and CTL Client plug-in utility installed on a computer that is running the Windows operating system.
For information about performing these tasks and about Cisco Unified Communications Manager security, refer to the *Cisco Unified Communications Manager Security Guide*.

Step 23 Perform a DRS backup on the publisher server to a remote SFTP server and verify that the backup succeeds. Record the DRS backup location and schedule information, if applicable.
To verify that your SFTP is working, use an SFTP client on a computer on the same subnet as the servers that are being restored and download the backup to that computer.

Ensure that all cluster nodes that you will replace or reinstall are online and registered as a node. DRS backs up only registered and online nodes.

You cannot perform this task if your old server is not working.

See the Create backup, on page 19.

- System configuration information, page 4
- Verify DNS registration, page 7
- Determine registration counts, page 8
- Record critical services, page 8
- Locate system errors, page 9
- Record trace log job details, page 9
- Record CDR management configuration, page 10
- Record system configuration counts, page 10
- Record firmware information, page 11
- Record system version, page 12

System configuration information

Before replacing or reinstalling a server, you must have the information that is described in this section. The information that is provided must match before and after the restore or reinstall. In the case of a server replacement, this information must match on both the original server and its replacement.

Gather this information for each Cisco Unified Communications Manager server that you are replacing or reinstalling in the cluster. You may not need to obtain all the information; gather only the information that is pertinent to your system and network configuration.

Account names and passwords record

Record all system passwords and account IDs, including those described in the following table. You cannot retrieve these passwords from the server.

Caution You must enter identical passwords and account IDs when you configure the replacement server.

If you replace a server that was previously upgraded from an older product release, your passwords might get denied by the Cisco Unified Communications Manager installation program. This happens because the password validation rules might get stronger in the new product release, but passwords do not get re validated during an upgrade. But when you perform a fresh installation on the server that you are replacing, the new, stronger password validation occurs.

If this happens, choose new passwords that the installation program will accept. For more information about passwords, see the document *Installing Cisco Unified Communications Manager*.

Table 2: Password and Accounts Configuration Data

Field	Description
Administrator ID: _____	The user ID that you use for secure shell access to the CLI, for logging into Cisco Unified Communications Manager Administration, and for logging into the Disaster Recovery System.
Administrator Password _____	The password that you use to log into the Administrator ID account.
Application User Name _____	The default Application User name for applications that are installed on the system, including Cisco Unified Communications Manager and Cisco Unified Serviceability. In 5.x releases, the Application User Name is set automatically during installation to CCMAdministrator. In 6.x releases, you choose the Application User Name during installation.
Application User Password _____	The password that is used as the default password for applications that are installed on the system, including Cisco Unified Communications Manager Administration and Cisco Unified Serviceability.

Field	Description
Security Password: _____	The security password that Cisco Unified Communications Manager servers in the cluster use to communicate with one another. You must enter the same password for all nodes in the cluster.

Record network configuration settings

Follow this procedure to record network configuration settings.

Caution You must enter identical network settings when you configure the replacement server. Do not attempt to change network settings on the replacement server. The only exceptions are the NIC speed and duplex settings, which you should configure as described in this section.

Procedure

Step 1 In Cisco Unified Communications Operating System Administration, navigate to **Show** > **Network**.

Step 2 Record all network configuration settings, including those described in the following table.

Table 3: Network Configuration Information

Parameter and Your Entry	Description
DHCP status: _____	Dynamic Host Configuration Protocol status. If DHCP is not enabled, you must enter a hostname, IP Address, IP Mask, and Gateway.
DNS Enabled: _____	DNS status. When DNS is not enabled, you should only enter IP addresses (not hostnames) for all network devices in your Cisco Unified Communications network.
DNS Primary: _____._____._____._____	The IP address of the primary DNS server that Cisco Unified Communications Manager contacts first when it attempts to resolve host names. Consider this setting as required if DNS is enabled.
DNS Secondary: _____._____._____._____	The IP address of the secondary DNS server that Cisco Unified Communications Manager will attempt to connect if the primary DNS server fails.
Domain: _____	The name of the domain in which this machine is located. Consider this setting as required if DNS is enabled.

Parameter and Your Entry	Description
Gateway Address: _____._____._____._____	The IP address of the default gateway, which is a network point that acts as an entrance to another network. Outbound packets get sent to the gateway that will forward them to their final destination. If you do not have a gateway, you must still fill in this field by setting it to 255.255.255.255. Not having a gateway may limit you to communicating only with devices on your subnet.
Hostname: _____	A name that represents an alias that is assigned to an IP address to identify it. Consider this setting as required if DHCP is disabled.
IP Address: _____._____._____._____	The IP address of this machine. It uniquely identifies the server on this network. Ensure that another machine in this network is not using this IP address. Consider this setting as required is DHCP is disabled.
IP Mask: _____._____._____._____	The IP subnet mask of this machine. The subnet mask together with the IP address defines the network address and the host address.
NIC Speed: _____	The speed of the server network interface card (NIC) in megabits per second.
NIC Duplex: _____	The duplex setting of the server NIC.
MTU size	Maximum transmission unit (MTU): the largest packet, in bytes, that this host will transmit on the network.
NTP Server: _____ _____._____._____._____	The hostname or IP address of the NTP server(s) with which you want to keep time synchronization. Consider this setting as required if you enabled the system to be an NTP client.

Step 3 Record the NIC speed and duplex settings of the switch port to which you will connect the new server. You should configure the same NIC settings on the server and on the switch port. For GigE (1000/FULL), you should set both NIC and switch port settings to Auto/Auto; do not set hard values.

If you are using Network Fault Tolerance, the Network Fault Tolerance configuration gets lost during the replacement. You will need to configure it on each server after the upgrade.

Enable PortFast on all switch ports that are connected to Cisco Unified Communications Manager servers. With Portfast enabled, the switch immediately brings a port from the blocking state into the forwarding state by eliminating the forwarding delay (the time that a port waits before changing from its Spanning-Tree Protocol (STP) learning and listening states to the forwarding state).

Related Topics

Before you begin, on page 1

Record SMTP settings

Follow this procedure to record the SMTP server setting, which specifies the hostname or IP address of the SMTP host that is used for outbound e-mail.

Procedure

Step 1 In Cisco Unified Communications Operating System Administration, navigate to **Settings** > **SMTP**.

Step 2 Record IP address or hostname of the SMTP server.

Record the hostname and timezone

Follow this procedure to record the hostname and timezone settings.

Procedure

Step 1 In Cisco Unified Communications Operating System Administration, navigate to **Show** > **System**.

Step 2 Record the settings in the following fields:

- Host Name - The unique host name of the server
- Time Zone - The local time zone and offset from Greenwich Mean Time (GMT)

Verify DNS registration

If you use DNS, verify that all servers to be replaced are registered in DNS properly.

Procedure

Step 1 Open a command prompt.

Step 2 To ping each server by its DNS name, enter:

ping *DNS name*

Step 3 To look up each server by IP address, enter:

nslookup *IP address*

Related Topics

Before you begin, on page 1

Determine registration counts

Record the number of registered devices, including the numbers of registered phones and gateways, by using the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT).

Procedure

Step 1 Download and install the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT) by choosing **Application** > **Plugins** from Cisco Unified Communications Manager Administration, clicking **Find**, and clicking the **Download** link next to the appropriate RTMT installer.
If you are planning to install the RTMT tool on a computer that is running the Microsoft Windows operating system, click the **Download** link for the Cisco Unified Communications Manager Real Time Monitoring Tool-Windows. If you are planning to install the RTMT tool on a computer that is running the Linux operating system, click the **Download** link for the Cisco Unified Communications Manager Real Time Monitoring Tool-Linux.

Step 2 Open RTMT.

Step 3 Perform one of the following tasks:

- In the Quick Launch Channel, click the **CallManager** tab, click the **View** tab, click the **Device** category, and click the **Device** icon.
- Choose **CallManager** > **Monitor** > **Device Summary**.

Step 4 For each Cisco Unified Communications Manager node, record the number for each device type that is displayed, including the numbers of registered phones, FXS, FXO, T1Cas, PRI, MOH, MTP, CFB, XCODE, and H323 Gateways.

Related Topics

Before you begin, on page 1
Complete replacement, on page 32

Record critical services

Record all the critical services and their status by using the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT).

Procedure

Step 1 Perform one of the following tasks:

- In the Quick Launch Channel, click the **System** tab, click the **View** tab, click the **Server** category, and click the **Critical Services** icon.
- Choose **System** > **Server** > **Critical Services**.

Step 2 Record the status of all critical services for each node in the cluster.

Related Topics

Before you begin, on page 1
Complete replacement, on page 32

Locate system errors

Using the Syslog viewer in the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT), locate any events that have a severity of Error or higher.

Procedure

Step 1 Open RTMT and perform one of the following tasks:

- In the Quick Launch Channel, click the **System** tab, click the **Tools** tab; then click the **SysLog Viewer** icon.
- Choose **System** > **Tools** > **SysLog Viewer** > **Open SysLog Viewer**.

Step 2 From the Select a Node drop-down list box, choose the server where the logs that you want to view are stored.

Step 3 Double-click the **Application Logs** folder.

Step 4 Locate events with a severity of Error or higher.

Step 5 Review each log to locate system-affecting errors.

Related Topics

Before you begin, on page 1
Complete replacement, on page 32

Record trace log job details

Record the details of all Trace and Log Central jobs.

Procedure

Step 1 Open RTMT and perform one of the following tasks:

- In the Quick Launch Channel, click the **System** tab, click the **Tools** tab; then, click the **Job Status** icon.
- Choose **System** > **Tools** > **Trace** > **Job Status**.

Step 2 Double click each scheduled job and record the details that display for each job in the Show Detail dialog box.

Related Topics

Before you begin, on page 1

Record CDR management configuration

Record CDR Management configuration and destinations, if applicable.

You use the CDR Management Configuration window to set the amount of disk space to allocate to call detail record (CDR) and call management record (CMR) files, configure the number of days to preserve files before deletion, and configure up to three billing application server destinations for CDRs. The CDR repository manager service repeatedly attempts to deliver CDR and CMR files to the billing servers that you configure on the CDR Management Configuration window until it delivers the files successfully, until you change or delete the billing application server on the CDR Management Configuration window, or until the files fall outside the preservation window and are deleted.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **CDR Management**.
The CDR Management Configuration window displays.

Step 2 Record the General Parameters and the Billing Application Server Parameters.

Related Topics

Before you begin, on page 1

Record system configuration counts

From Cisco Unified Communications Manager Administration, obtain counts of each of the items that are configured on the system that you want to verify after the replacement. Some examples of items to count follow:

- Phones

- Gateways
- Trunks
- Users
- Route patterns
- CTI ports
- CTI route points

Procedure

Step 1 In Cisco Unified Communications Manager Administration, access the windows for each item that you want to count and click **Find** without entering any search parameters. Some examples follow:

- Find and List Phones (**Device** > **Phone**)
- Find and List Gateway (**Device** > **Gateway**)
- Find and List Trunks (**Device** > **Trunk**)
- Find and List Route Patterns (**Call Routing** > **Route/Hunt** > **Route Pattern**)
- Find and List Users (**User Management** > **End Users**)
- Find and List Application Users (**User Management** > **Application Users**)

Step 2 Record the number of each of the items (devices, route patterns, and users).

Related Topics

Before you begin, on page 1
Complete replacement, on page 32

Record firmware information

Record all of the phone loads and device types that display on the Firmware Load Information window.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Firmware Load Information**.
The Firmware Load Information window displays.

Step 2 Record all the phone loads and device types that display.

Note If you have custom device types that do not ship with Cisco Unified Communications Manager, make sure that you have the appropriate COP files, so you can reinstall them.

Related Topics

Before you begin, on page 1
Complete replacement, on page 32

Record system version

Compare the system version on each node in your cluster by using Cisco Unified Communications Operating System Administration.

Verify that you have DVDs with that version. If you have a service release, you need media for base image and the service release.

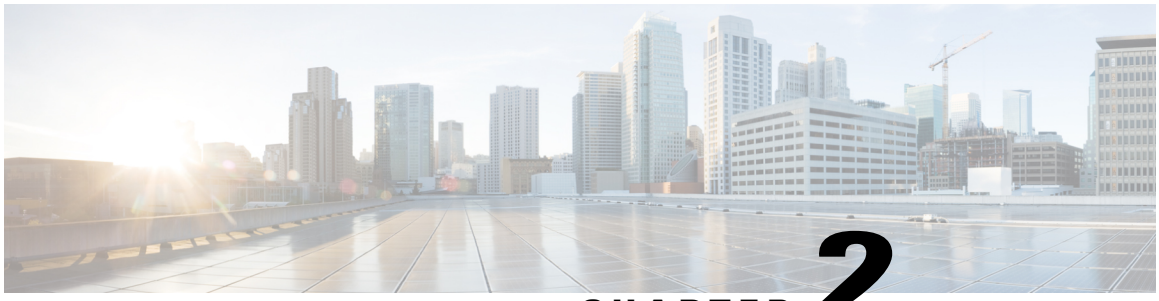
Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Show** > **System**.
The System Status window displays.

Step 2 Make a note of the value that is displayed in the Product Version field.

Related Topics

Before you begin, on page 1
Complete replacement, on page 32



CHAPTER 2

Replace single server or cluster

Caution Because this process is designed to work as a server replacement, you must perform it in the live environment. Cisco does not recommend doing this process on a "dead net" because a duplication of entire network environment is required, which is highly risky.

This section provides checklists of the steps that are required to replace a single server or a cluster:

- If you are replacing an entire cluster, replace the servers in the order that is described in the following steps.
- If you are replacing a publisher node in a cluster, or a single server that is not part of a cluster, go to the applicable procedure.
- If you are replacing one or more subscriber nodes or dedicated TFTP servers, go to the applicable procedure.

Procedure

Step 1 Replace the publisher node.

Step 2 Replace any dedicated TFTP servers or other non-Cisco Unified Communications Manager cluster nodes.

Step 3 Replace all backup subscriber nodes.

Step 4 Replace all primary subscriber nodes.

Step 5 Perform any remaining post-replacement tasks.

- Replace publisher node, page 14
- Replace subscriber or dedicated TFTP server, page 15
- Upgrade vSphere ESXi, page 16
- Migrate from single to multi-vDisk virtual machine, page 16
- Change virtual machine configuration specifications, page 17

Replace publisher node

Complete the following tasks to replace the Cisco Unified Communications Manager publisher server. If you are replacing a single server that is not part of a cluster, follow this procedure to replace your server.

Note A new license file is required if you are installing a replacement motherboard in publisher servers or single servers that are not part of a cluster.

Procedure

Step 1 Perform the preparatory tasks.

Step 2 Gather the necessary information about the old publisher server.

Step 3 Back up the publisher server to a remote SFTP server by using Disaster Recovery System (DRS) and verify that you have a good backup.

Step 4 Get new licenses of all the license types before system replacement.
Get new licenses of all the license types: Software License Feature, CCM Node License Feature, and Phone License Feature.

You only need a new license if you are replacing the publisher node.

Step 5 Shut down and turn off the old server.

Step 6 Connect the new server.

Step 7 Install the same Cisco Unified Communications Manager release on the new server that was installed on the old server, including any Engineering Special releases. Configure the server as the publisher server for the cluster.

Step 8 Restore backed-up data to the publisher server by using DRS.

Step 9 Reboot all nodes in the cluster, starting with the subscriber nodes. Reboot the publisher node after all subscriber nodes finish rebooting. If the server is not in a cluster, then reboot the server.

Step 10 Upload all of the new license files to the publisher server.
Upload new license files for all of the license types: Software License Feature, CCM Node License Feature, and Phone License Feature.

Step 11 Delete all invalid license files (those based on the old server MAC address).

Step 12 Perform the post-replacement tasks.

Related Topics

Before you begin, on page 1
System configuration information, on page 4
Create backup, on page 19
Obtain license file, on page 23
Install software on publisher server, on page 23
Restore backup file, on page 30
Upload license file, on page 29

Delete invalid license files
Complete replacement, on page 32

Replace subscriber or dedicated TFTP server

Complete the following tasks to replace a subscriber node or dedicated TFTP server (or another server type that is not a Cisco Unified Communications Manager server). A dedicated TFTP server is a node with Cisco Unified Communications Manager installed but with the Cisco Unified Communications Manager service disabled. The TFTP service runs as a dedicated TFTP server for the cluster.

If you are also replacing the publisher node, you must replace it before replacing or reinstalling any other nodes. If the cluster uses backup subscriber nodes, replace or reinstall all backup subscriber nodes before replacing or reinstalling primary subscriber nodes.

You can replace all backup subscriber nodes at the same time if this does not cause outages or oversubscription of primary subscriber nodes. You can replace all primary subscriber nodes at the same time if this does not cause outages or oversubscription of backup subscriber nodes.

Follow the references in the For More Information column to get more information about a step.

Procedure

Step 1 Gather the necessary information about the old server.

Step 2 If you are getting the system time from an NTP server, verify that the publisher node can synchronize with the NTP server before you install a subsequent node.

Step 3 Shut down and turn off the old server.

Step 4 Connect the new server.

Step 5 Install the same Cisco Unified Communications Manager release on the new server that was installed on the old server, including any Engineering Special releases. Configure the new server to use the same configuration information as the old server.

Step 6 Restore backed up data to the node by using DRS.

Step 7 Reboot the new server.

Step 8 Verify that the new server has the same number and status for all Critical services that you gathered before replacing the server.

Step 9 Verify that the db Replicate state has a value of 2. This indicates that the database is set up on this node.

Step 10 Perform the post-replacement tasks.

Related Topics

Replace single server or cluster, on page 13
System configuration information, on page 4
Verify NTP status, on page 23
Install software on subscriber server, on page 26
Restore backup file, on page 30
Before you begin, on page 1
Complete replacement, on page 32

Replace publisher node, on page 14
Replace subscriber or dedicated TFTP server, on page 15

Upgrade vSphere ESXi

Use the following procedure when you need to update your vSphere ESXi hypervisor in order to upgrade to a new release of Unified Communications Manager.

Procedure

Step 1 Move the virtual machine that is running Unified Communications Manager off the host server using one of the following methods:

- If you have a hot standby host, use vMotion to migrate the virtual machine from one physical server to another.
- If you do not have a hot standby host, power down the virtual machine and copy it to a different location.

Step 2 Upgrade the vSphere ESXi using the upgrade procedures provided by VMware.

Step 3 Verify that the vSphere ESXi upgraded successfully.

Step 4 Move the virtual machine that is running Unified Communications Manager back to the host server using one of the following methods:

- If you have a hot standby host, use vMotion to migrate the virtual machine from one physical server to another.
- If you do not have a hot standby host, power down the virtual machine and copy it the host server.

What to Do Next

If you need to update the virtual machine version or the VMware compatibility version in order to upgrade the vSphere ESXi, proceed to Change virtual machine configuration specifications, on page 17

Migrate from single to multi-vDisk virtual machine

If you are migrating to a larger virtual machine (VM) deployment that requires multiple vDisks, perform the following procedure. After you complete this procedure, you must Change virtual machine configuration specifications, on page 17 to ensure that the specifications match the requirements of the release.

Procedure

Step 1 Perform a backup of the existing virtual machine (VM).

Step 2 Power off the existing VM and remove it from the network.

Step 3 Deploy a new VM at the correct user count using the appropriate OVA template.

Step 4 Perform a fresh installation of the same software release of IM and Presence or Cisco Unified Communications Manager on the new VM using the same hostname and IP address.

Step 5 Perform a DRS restore on the new VM.

Change virtual machine configuration specifications

Use the following procedure when you need to change the configuration specifications on your virtual machine (VM) in order to upgrade to a new release of Unified Communications Manager or IM and Presence Service. Configuration specifications include the vCPU, vRAM, and vDisk size. For information about VM requirements, see the Readme file with the OVA template that supports your release. Details about OVA templates are available on the Virtualization Docwiki at http://docwiki.cisco.com/wiki/Implementing_Virtualization_Deployments.

Procedure

Step 1 Perform a Disaster Recovery System (DRS) backup.
For more information about performing a backup, see the *Cisco Unified Communications Manager Disaster Recovery Administration Guide.*

Step 2 (Optional.) If you need to increase the vDisk space to meet the space requirements of a refresh upgrade, install the following COP file:
`ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn`

Step 3 Change the configuration of the virtual machine as needed:

a) Change the Guest OS version to match the requirements of the new release.
b) To change the vCPU, make the change in vSphere Client. Ensure that you change the reservation value to match the specifications of the new release.
c) To change the vRAM, make the change in vSphere Client. Ensure that you change the reservation value to match the specifications of the new release.
d) To increase the vDisk space, edit the disk size using vDisk. If the virtual machine has two disks, expand the second one.
The new space is automatically added to the common partition when you restart the virtual machine.

Note You need to change the disk size changes only if you need additional space to complete the upgrade. The disk space requirements are specified in the Readme file for the OVA template.

For more information about making configuration changes using vSphere Client, refer to the user manual for the product.

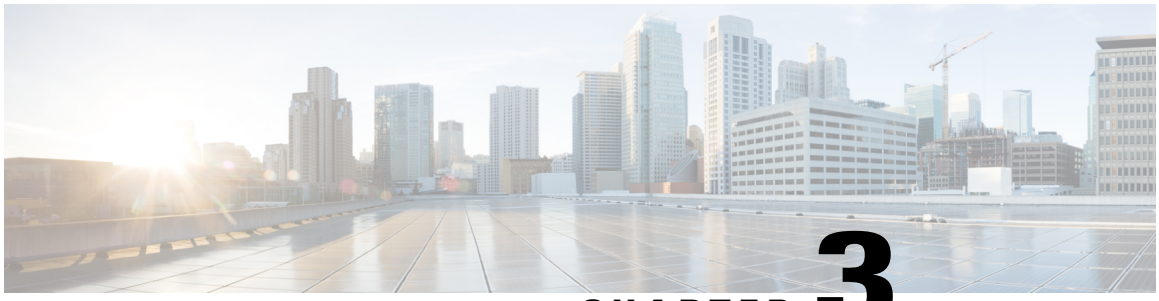
Step 4 Modify the Network Adapter to use the VMXNET 3 Adapter type.

For information about modifying the Network Adapter to meet the requirements of this release, see the Readme file for the OVA template.

Step 5 Upgrade the software to the latest version.

Step 6 Shut down the virtual machine.

Step 7 Power on the virtual machine.



CHAPTER 3

Complete replacement

- Create backup, page 19
- Obtain license file, page 23
- Verify NTP status, page 23
- Install software on publisher server, page 23
- Install software on subscriber server, page 26
- Upload license file, page 29
- Restore backup file, page 30
- Complete replacement, page 32
- Upgrade server hardware, page 33

Create backup

The following sections describe how to set up and run a backup before an upgrade. Refer to the *Disaster Recovery System Administration Guide* for more information.

If you are recovering or replacing a server, you can skip this section on creating backups and restore the server from the most recent backup that is available.

Related Topics

Replace publisher node, on page 14
Replace subscriber or dedicated TFTP server, on page 15

Supported features and components

You can back up and restore the features and subcomponents that are shown in the following table. For each feature that you choose, the system backs up all its subcomponents automatically.

Table 4: Supported Features and Components

Feature	Components
CCM - Cisco Unified Communications Manager	Cisco Unified Communications Manager database (CMDB)
	Platform
	Cisco Unified Serviceability
	Music On Hold (MOH)
	Cisco Emergency Responder (CER)
	Bulk Tool (BAT)
	Preference
	Phone device files (TFTP)
	syslogagt (SNMP syslog agent)
	cdpagent (SNMP cdp agent)
	tct (trace collection tool)
	Call Detail Records (CDR)
	CDR Analysis and Reporting (CAR)

Configure features for backup

Before you can schedule or start a backup job, you must configure the features that you want to back up.

Note Changing a backup feature changes it for both manual and scheduled backups.

Perform the following steps to choose the features that you want to back up.

Procedure

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose Disaster Recovery System from the Navigation menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator user name and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Backup** > **Configure Features**.

Step 4 From the list of available features, choose the feature or features that you want to include in the backup and click **Save**. You must choose at least one feature.

Step 5 Continue with the next procedure for configuring a storage location.

Configure storage location

Before using the Disaster Recovery System, you must configure the location where you want the backup file to be stored. Perform the following steps to configure the storage location.

Procedure

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator user name and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Backup** > **Storage Location**. The Storage Location window displays.
Note You can configure the number of backup sets that are stored on a network directory.

Step 4 Select the Network Directory option to store the backup data on a networked drive that is accessed through an SFTP connection.

Step 5 Enter the following required information:

- Server name: Name or IP address of the network server
- Path name: Path name for the directory where you want to store the backup file
- User name: Valid username for an account on the remote system
- Password: Valid password for the account on the remote system

Note You must have access to an SFTP server to configure a network storage location. The SFTP path must exist prior to the backup. Ensure that the account that is used to access the SFTP server has write permission for the selected path.

Step 6 To update these settings, click **Save**.
Note For network directory backups, after you click the Save button, the DRS Master Agent will validate the selected SFTP server. If the user name, password, server name, or directory path is invalid, the save will fail.

Step 7 Continue with either a manual or a scheduled backup.

Start backup

You can manually start a backup of the features that you choose on the Configure Features menu. Perform the following steps to start a manual backup.

Procedure

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator user name and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Backup** > **Manual Backup**. The Manual Backup window displays.

Step 4 Make sure the features that you want to back up are chosen. To choose other features, see the Configure features for backup, on page 20.

Note Ensure all servers in the cluster are running the same version of Cisco Unified Communications Manager and are reachable through the network. Servers that are not running at the time of the scheduled backup will not get backed up.

Step 5 To begin the manual backup, click **Start Backup**.

Step 6 Make sure that you have configured the backup storage location. See the Configure storage location, on page 21.

Check backup status

Perform the following steps to check the status of the current backup job.

Procedure

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator user name and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Backup** > **Current Status**. The Backup Status window displays.

Step 4 To view the backup log file, click the log filename link.

Step 5 To cancel the current backup, click **Cancel Backup**.

Note The backup cancels after the current component completes its backup operation.

Obtain license file

If you have to replace the first node in your Cisco Unified Communications Manager cluster, you must open a case with the licensing team to obtain a license for your replacement server. Contact the licensing team at licensing@cisco.com. After you receive the new license file, upload the software license file.

Note Replacing a motherboard on the first node also requires a new license file.

Related Topics

Upload license file, on page 29
Replace publisher node, on page 14

Verify NTP status

If you are getting the system time from an NTP server, verify that the publisher node can synchronize with the NTP server before you install a subscriber node.

To verify the NTP status of the first node, log into the command line interface on the publisher node and enter the following command:

utils ntp status

For more information, see the *Cisco Unified Communications Operating System Administration Guide*.

Caution If the first node fails to synchronize with an NTP server, installation of a subsequent node can also fail.

Install software on publisher server

Use this procedure to install Cisco Unified Communications Manager on the new publisher server. For more information about installing this product, refer to the document, *Installing Cisco Unified Communications Manager*.

Procedure

Step 1 Insert the installation DVD into the tray and restart the server, so it boots from the DVD. After the server completes the boot sequence, the DVD Found window displays.

Step 2 To perform the media check, choose **Yes** or, to skip the media check, choose **No**.
The media check checks the integrity of the DVD. If your DVD passed the media check previously, you might choose to skip the media check.

Step 3 If you choose **Yes** to perform the media check, the system installer performs the media check and displays the Media Check Result window. Perform these tasks:

a) If the Media Check Result displays Pass, choose **OK** to continue the installation.
b) If the media fails the media check, either download another copy of the software from Cisco.com or obtain another disc directly from Cisco.

Step 4 The system installer performs the following hardware checks to ensure that your system is correctly configured. If the installer makes any changes to your hardware configuration settings, you will get prompted to restart your system. Leave the DVD in the drive during the restart.

- First, the installation process checks for the correct drivers, and you may see the following warning:

```
No hard drives have been found. You probably need to manually
choose device drivers for install to succeed.
Would you like to select drivers now?
```

  To continue the installation, choose **Yes.**

- The installation next checks to see whether you have a supported hardware platform. If your server does not meet the exact hardware requirements, the installation process fails with a critical error. If you think this is not correct, capture the error and report it Cisco support.
- The installation process next verifies RAID configuration and BIOS settings.

  Note If this step repeats, choose **Yes** again.

After the hardware checks complete, the Product Deployment Selection window displays.

Step 5 In the Product Deployment Selection window, select Cisco Unified Communications Manager; then, choose **OK.**

Step 6 If software is currently installed on the server, the Overwrite Hard Drive window opens and displays the current software version on your hard drive and the version on the DVD. To continue with the installation, choose **Yes**, or choose **No** to cancel.

Caution If you choose **Yes** on the Overwrite Hard Drive window, all existing data on your hard drive gets overwritten and destroyed.

Step 7 The Platform Installation Wizard window displays.

Step 8 To configure the platform now, choose **Proceed.**

Step 9 In the Basic Install window, choose **Continue** to install the software version on the DVD.

Step 10 When the Timezone Configuration displays, choose the appropriate time zone for the server and then choose **OK**.
The Auto Negotiation Configuration window displays.

Step 11 The installation process allows you to automatically set the speed and duplex settings of the Ethernet network interface card (NIC) by using automatic negotiation. You can change this setting after installation.

- To enable automatic negotiation, choose **Yes**.

  The MTU Configuration window displays.

  Note To use this option, your hub or Ethernet switch must support automatic negotiation.

- To disable automatic negotiation, choose **No** and continue with the next step.

  The NIC Speed and Duplex Configuration window displays.

Step 12 If you chose to disable automatic negotiation, manually choose the appropriate NIC speed and duplex settings now and choose **OK** to continue.
The MTU Configuration window displays.

Step 13 In the MTU Configuration window, you can change the MTU size from the operating system default.
The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value, which is 1500 bytes.

Caution Configuring the MTU size incorrectly can affect your network performance.

- To accept the default value (1500 bytes), choose **No.**
- To change the MTU size from the operating system default, choose **Yes**, enter the new MTU size, and choose **OK.**

The DHCP Configuration window displays.

Step 14 For network configuration, you can choose to either set up static network IP address for the node or to use Dynamic Host Configuration Protocol (DHCP).

- If you have a DHCP server that is configured in your network and want to use DHCP, choose **Yes**.

  The Administrator Login Configuration window displays.
- If you want to configure static IP address for the node, choose **No** and continue with the next step.

  The Static Network Configuration window displays.

Step 15 If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See Record network configuration settings, on page 5 for field descriptions.
The DNS Client Configuration window displays.

Step 16 To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See Record network configuration settings, on page 5 for field descriptions.
The Administrator Login Configuration window displays.

Step 17 Enter your Administrator login and password from Account names and passwords record, on page 4.
The Certificate Signing Request Information window displays.

Step 18 Enter your certificate signing request information and choose **OK.**
The First Node Configuration window displays.

Step 19 To configure this server as the first Cisco Unified Communications Manager node, choose **Yes.**
The Network Time Protocol Client Configuration window displays.

Step 20 Choose whether you want to configure an external NTP server or manually configure the system time.

Note Cisco recommends that you use an external NTP server to ensure accurate system time on the first node. Ensure the external NTP server is stratum 9 or higher (meaning stratums 1-9). Subsequent nodes in the cluster will get their time from the first node.

- To set up an external NTP server, choose **Yes** and enter the IP address, NTP server name, or NTP server pool name for at least one NTP server. You can configure up to five NTP servers, and Cisco recommends that you use at least three. Choose **Proceed** to continue with the installation.

  The system contacts an NTP server and automatically sets the time on the hardware clock.

Note If you already entered the network configuration information and the system rebooted (a Skip installation), the **Test** button displays. You can choose **Test** to check whether the NTP servers are accessible.

- To manually configure the system time, choose **No** and enter the appropriate date and time to set the hardware clock. Choose **OK** to continue with the installation.

The Database Access Security Configuration window displays.

Step 21 Enter the Database Access Security password from Account names and passwords record, on page 4.
The SMTP Host Configuration window displays.

Step 22 If you want to configure an SMTP server, choose **Yes** and enter the SMTP server name.
Note You must configure an SMTP server to use certain platform features; however, you can also configure an SMTP server later by using the operating system GUI or the command line interface.

Step 23 Choose **OK.**
The Platform Configuration Confirmation window displays.

Step 24 To continue with the installation, choose **OK.**
The Application User Password Configuration window displays.

Note If you need to change one of your previous entries, choose **Back**, make the change, and continue with the installation.

Step 25 Enter the Application User Password from Account names and passwords record, on page 4 and confirm the password by entering it again.

Step 26 Choose **OK.**
The system installs and configures the software. The DVD drive ejects, and the server reboots. Do not reinsert the DVD.

Step 27 When the installation process completes, you get prompted to log in by using the Administrator account and password.

Step 28 Complete the rest of the tasks that are listed in the Replace publisher node, on page 14.

Install software on subscriber server

Use this procedure to install Cisco Unified Communications Manager on a new subscriber server.

Procedure

Step 1 If you configured Network Time Protocol (NTP) on the publisher node, ensure that the publisher node is synchronized with an NTP server before you install a subscriber node. From the Command Line Interface on the publisher node, enter the command **utils ntp status**. Ensure that the printout indicates that the node is synchronized with an NTP server.
Note If the first node is not synchronized with an NTP server, installation of the subsequent node will fail.

Step 2 Insert the installation DVD into the tray and restart the server, so it boots from the DVD. After the server completes the boot sequence, the DVD Found window displays.

Step 3 To perform the media check, choose **Yes** or, to skip the media check, choose **No.**

The media check checks the integrity of the DVD. If your DVD has passed the media check previously, you might choose to skip the media check.

Step 4 If you choose **Yes** to perform the media check, the system installer performs the media check and displays the Media Check Result window. Perform these tasks:

a) If the Media Check Result displays Pass, choose **OK** to continue the installation.
b) If the media fails the media check, either download another copy of the software from Cisco.com or obtain another disc directly from Cisco.

Step 5 The system installer performs the following hardware checks to ensure that your system is correctly configured. If the installer makes any changes to your hardware configuration settings, you will get prompted to restart your system. Leave the DVD in the drive during the reboot.

- First, the installation process checks for the correct drivers, and you may see the following warning:

```
No hard drives have been found. You probably need to manually
choose device drivers for install to succeed.
Would you like to select drivers now?
```

  To continue the installation, choose **Yes.**

- The installation next checks to see whether you have a supported hardware platform. If your server does not meet the exact hardware requirements, the installation process fails with a critical error. If you think this is not correct, capture the error and report it Cisco support.
- The installation process next verifies RAID configuration and BIOS settings.

  Note If this step repeats, choose **Yes** again.

After the hardware checks complete, Product Deployment Selection window displays.

Step 6 In the Product Deployment Selection window, select Cisco Unified Communications Manager; then, choose **OK.**

Step 7 If software is currently installed on the server, the Overwrite Hard Drive window opens and displays the current software version on your hard drive and the version on the DVD. Choose **Yes** to continue with the installation or **No** to cancel.

Caution If you choose Yes on the Overwrite Hard Drive window, all existing data on your hard drive gets overwritten and destroyed.

Step 8 The Platform Installation Wizard window displays.

Step 9 To configure the platform now, choose **Proceed.**

Step 10 In the Basic Install window, choose **Continue** to install the software version on the DVD.

Step 11 When the Timezone Configuration displays, choose the appropriate time zone for the server and then choose **OK**.
The Auto Negotiation Configuration window displays.

Step 12 The installation process allows you to automatically set the speed and duplex settings of the Ethernet network interface card (NIC) by using automatic negotiation. You can change this setting after installation.

- To enable automatic negotiation, choose **Yes**.

  The MTU Configuration window displays.

  Note To use this option, ensure that your hub or Ethernet switch supports automatic negotiation.

- To disable automatic negotiation, choose **No** and continue with the next step.

  The NIC Speed and Duplex Configuration window displays.

Step 13 If you chose to disable automatic negotiation, manually choose the appropriate NIC speed and duplex settings now and choose **OK** to continue.
The MTU Configuration window displays.

Step 14 In the MTU Configuration window, you can change the MTU size from the operating system default.
The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value, which is 1500 bytes.

Caution Configuring the MTU size incorrectly can affect your network performance.

- To accept the default value (1500 bytes), choose **No.**
- To change the MTU size from the operating system default, choose **Yes**, enter the new MTU size, and choose **OK.**

The DHCP Configuration window displays.

Step 15 For network configuration, you can choose to either set up static network IP address for the node or to use Dynamic Host Configuration Protocol (DHCP).

- If you have a DHCP server that is configured in your network and want to use DHCP, choose **Yes**.

  The Administrator Login Configuration window displays.

- If you want to configure static IP address for the node, choose **No** and continue with the next step.

  The Static Network Configuration window displays.

Step 16 If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See Record network configuration settings, on page 5 for field descriptions.
The DNS Client Configuration window displays.

Step 17 To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See Record network configuration settings, on page 5 for field descriptions.
The Administrator Login Configuration window displays.

Step 18 Enter your Administrator login and password from Account names and passwords record, on page 4.
The Certificate Signing Request Information window displays.

Step 19 Enter your certificate signing request information and choose **OK.**
The First Node Configuration window displays.

Step 20 To configure this server as a subsequent node in the cluster, choose **No.**
The First Node Configuration window displays.

Caution You must configure a subsequent node on the first node by using Cisco Unified Communications Manager Administration before you install the subsequent node. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

Step 21 On the First Node Configuration window, read the Warning and make sure that you have correctly configured the first node. To continue with the installation of the subsequent node, choose **OK.**
The Network Connectivity Test Configuration window displays.

Step 22 During installation of a subsequent node, the system checks to ensure that the subsequent node can connect to the first node.

- To pause the installation after the system successfully verifies network connectivity, choose **Yes.**
- To continue the installation with a pause, choose **No.**

The First Node Access Configuration window displays.

Step 23 Enter the first node connectivity information to enable this subscriber node to connect to the subscriber node. If you chose to pause the system after the system successfully verified network connectivity, the Successful Connection to First Node window displays. Choose **Continue.**

Note If the network connectivity test fails, the system always stops and allows you to go back and reenter the parameter information.

The SMTP Host Configuration window displays.

Step 24 If you want to configure an SMTP server, choose **Yes** and enter the SMTP server name.

Note You must configure an SMTP server to use certain operating system features; however, you can also configure an SMTP server later by using the operating system GUI or the command line interface.

The Platform Configuration Confirmation window displays.

Step 25 To start installing the software, choose **OK**, or if you want to change the configuration, choose **Back.**

Step 26 When the installation process completes, you get prompted to log in by using the Administrator account and password.

Step 27 Complete the rest of the tasks in the Replace subscriber or dedicated TFTP server, on page 15.

Upload license file

Use the following procedure to upload a license file to the Cisco Unified Communications Manager server with the matching MAC address that is provided when a license file is requested. For information about obtaining a license file, see the Obtain license file, on page 23. The Cisco Unified Communications Manager server where the license file is loaded takes on the functionality of the license manager.

Note Upload the license file only on the first node of Cisco Unified Communications Manager cluster.

Procedure

Step 1 Choose **System** > **License** > **Upload License File**.
The License File Upload window displays.

Step 2 The Existing License Files drop-down list box displays the license files that are already uploaded to the server.

Note To view the file content of any existing files, choose the file from the drop-down list box and click **View File**.

Step 3 To choose a new license file to upload, click **Upload License File**.
The Upload File window displays.

Step 4 Browse and choose a license file to upload to the server.

Note The format of the license file that you receive specifies CCM<timestamp>.lic. If you retain the .lic extension, you can rename the license file. You cannot use the license if you edit the contents of the file in any way.

Step 5 Click **Upload License File**.
After the upload process completes, the Upload Result file displays.

Step 6 Click **Close.**

Step 7 In the License File Upload window, the status of the uploaded file displays.

Note The system uploads the license file into the database only if the version that is specified in the license file is greater than or equal to the Cisco Unified Communications Manager version that is running in the cluster. If the version check fails, an alarm occurs, and you should get a new license file with the correct version. The system bases the version check only on major releases.

Step 8 Restart the Cisco CallManager service. For information on restarting services, refer to the *Administration Guide for Cisco Unity Connection Serviceability*.

Related Topics

Replace publisher node, on page 14

Restore backup file

The Restore Wizard takes you through the steps that are required to restore a backup file. To perform a restore, use the procedure that follows.

Caution Before you restore Cisco Unified Communications Manager, ensure that the Cisco Unified Communications Manager version that is installed on the server matches the version of the backup file that you want to restore.

Procedure

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator user name and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Restore** > **Restore Wizard**. The Restore Wizard Step 1 window displays.

Step 4 Choose the Network Directory storage location from which you want to restore the file and enter the following required information for the chosen storage location:

- Server name: Name or IP address of the network server
- Path name: Path name for the directory from which you want to restore the backup data

- User name: Valid username for an SFTP account on the remote system
- Password: Valid password for the SFTP account on the remote system

Step 5 Click **Next**. The Restore Wizard Step 2 window displays.

Step 6 Choose the backup file that you want to restore.

Note The backup filename indicates the date and time that the system created the backup file.

Step 7 Click **Next**. The Restore Wizard Step 3 window displays.

Step 8 Choose the features that you want to restore.

Note Only the features that were backed up to the file that you chose display.

Step 9 Click **Next**. The Restore Wizard Step 4 window displays.

Step 10 To start restoring the data, click **Restore**.
You get prompted to choose the node to restore.

Step 11 Choose the appropriate node.

Caution After you choose the node to which you want the data restored, any existing data on that server gets overwritten.

Step 12 Your data gets restored on the nodes that you chose.

Note Depending on the size of your database and the components that you choose to restore, the system can require 1 hour or more to restore.

Related Topics

Replace publisher node, on page 14
Replace subscriber or dedicated TFTP server, on page 15
View restore status, on page 31

View restore status

To check the status of the current restore job, perform the following steps:

Procedure

Step 1 Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.
The Disaster Recovery System Logon window displays.

Step 2 Log in to the Disaster Recovery System by using the same Administrator user name and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Navigate to **Restore** > **Status**. The Restore Status window displays.

Step 4 To view the restore log file, click the log filename link.

Complete replacement

Perform the following tasks after you complete the cluster replacement:

Procedure

Step 1 If your server or cluster ran in secure mode, create a new CTL file and distribute it to all the cluster nodes. Do this step after you finish replacing or reinstalling all the servers that you intend to replace or reinstall. For information about performing these tasks and about Cisco Unified Communications Manager security, refer to the *Cisco Unified Communications Manager Security Guide*.

Caution You must create and distribute a new CTL file, or your secure phones will not work because they cannot register with the replaced Cisco Unified Communications Manager server(s).

Step 2 Using the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT), make sure that all the registration information values match the values that you recorded before the server replacement.

Step 3 Using the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT), make sure that all the critical services and their status match those that you recorded before the server replacement.

Step 4 Using the Syslog viewer in the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT), locate any events that have a severity of Error or higher. Perform this task to ensure that no system-affecting errors exist on your system.

Step 5 Using the Syslog viewer in the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT), check the Replicate_State counter for the Number of Replicates Created and State of Replication object on all nodes. The value on each node should equal 2.
This counter represents the state of replication, which includes the following possible values:

- 0 - Initializing. The counter equals 0 when the server is not defined or when the server is defined but the realize template has not completed.
- 1 - The system created replicates of some tables but not all tables. Cisco recommends that you run `utils dbreplication status` on the CLI to determine the location and cause of the failure.
- 2 - Good Replication.
- 3 - Bad Replication. When the counter displays a value of 3, consider replication in the cluster as bad. It does not mean that replication failed on a particular node. Cisco recommends that you run `utils dbreplication status` on the CLI to determine the location and cause of the failure.
- 4 - Replication setup did not succeed.

Step 6 To access the appropriate object and counter, use the following procedure:

a) Perform one of the following tasks:
   - In the Quick Launch Channel, click **System** > **Performance**; then, click the **Performance** icon.
   - Choose **Performance** > **Open Performance Monitoring**.

b) Double-click the name of the server where you want to add a counter to monitor.
c) Double-click the **Number of Replicates Created** and **State of Replication** object.
d) Double-click the **Replicate_State** counter.

e) Choose the **ReplicateCount** instance and click **Add.**

Step 7 From Cisco Unified Communications Manager Administration, make sure that the number of phones, gateways, trunks, users, and route patterns that are configured in the database matches the numbers that you recorded before the server replacement.

Step 8 From the Firmware Load Information window in Cisco Unified Communications Manager Administration, make sure that the phone load type value matches the value that you recorded before the server replacement.

Step 9 Reinstall the COP file enablers for any custom device types that do not ship with Cisco Unified Communications Manager. Then, reboot the cluster and start post-replacement checklist again.

Step 10 Reinstall any locales that were installed on the server.

Step 11 Compare the system version on each node in your cluster by using Cisco Unified Communications Operating System Administration and make sure that it matches the version that you recorded before the replacement.

Step 12 Reconfigure CDR destinations, if applicable.

Step 13 Reconfigure all Trace and Log Central jobs.

Step 14 Perform any system tests that you performed before the replacement and verify that all test calls succeed.

Step 15 Reconfigure DRS location and schedule, if applicable.

Related Topics

Record system configuration counts, on page 10
Determine registration counts, on page 8
Record critical services, on page 8
Locate system errors, on page 9
Record firmware information, on page 11
Record system version, on page 12
Record CDR management configuration, on page 10
Record trace log job details, on page 9
Create backup, on page 19

Upgrade server hardware

The following sections contain information about upgrading server hardware When Upgrading to Cisco Unified Communications Manager Release 8.6(1):

• Memory recommendations, on page 33
• Upgrade hard drives, on page 34

Memory recommendations

It is strongly recommended that you run Cisco Unified Communications Manager Release 8.6(1) only on servers with at least 4 GB of memory.

Upgrade hard drives

Follow this procedure to replace 72 GB hard drives with 146 GB hard drives when you upgrade to Cisco Unified Communications Manager Release 8.6(1):

Procedure

Step 1 Reduce used disk space by following these steps:

a) Enter the CLI command **show status**.
If the active partition is 97% full or higher, seriously consider replacing the 72 GB drives with 146 GB drives. Use Real Time Monitoring Tool to monitor disk space usage.

b) If you are running Cisco Unified Communications Manager release 6.x or higher, reduce used disk space by performing these steps:

- Enter the CLI command **utils diagnose module disk_files** to identify files that you can delete.
- To delete files that you identified, use the CLI command **file delete**.
- Enter the CLI command **show status** to see the new disk space usage on the active partition.

Step 2 Back up the server using Disaster Recovery System.

Step 3 If you are running Cisco Unified Communications Manager release 5.x, upgrade the server to a 7.x release. If the upgrade fails, switch back to release 5.x and report the issue to Cisco Technical Support.

Step 4 Upgrade the server to release 8.6(1).

Step 5 If the upgrade to release 8.6(1) fails due to disk space shortage in /common, as reported by Real Time Monitoring Tool or in the upgrade log file (look for phrases with the word “space” in them, such as “Not enough space on partition to proceed” or “No space left on device”), perform the recommended workaround in Adjust logging, on page 35, then go back to the previous step.

a) If the server originally was running Cisco Unified Communications Manager release 5.x, perform a fresh installation of the same 5.x release, then restore the data using Disaster Recovery System, then go to the next step.

b) If the server was originally not running Cisco Unified Communications Manager release 6.x or higher and the switchover to release 8.6(1) occurred, then clean up disk space using the procedure in the first step, then switch back to the previous release.

c) Order 146 GB hard drives.

d) When the new hard drives are ready to be installed, perform these steps:

- Perform a backup of the existing Cisco Unified Communications Manager release using Disaster Recovery System.
- Install the new hard drives
- Perform a fresh installation of the existing Cisco Unified Communications Manager release.
- Restore data to the server using Disaster Recovery System.
- Continue with upgrading the server.

Step 6 If the upgrade to release 8.6(1) fails for other reasons, contact Cisco Technical Support.

Step 7 If the upgrade to release 8.6(1) succeeds, be sure to run Real Time Monitoring Tool and monitor disk space usage, particularly if the active partition found in this procedure was already over 97% disk usage.

Adjust logging

To change one of the values below, click the right mouse button on the attribute and select Set Alert/Properties. Once in the dialog box, click **Next** to open the dialog box for modifying the threshold values.

Before the upgrade:

Procedure

Step 1 Launch Real Time Monitoring Tool.

Step 2 Select Alert Central, then perform the following tasks:

a) Select LogPartitionHighWaterMarkExceeded, note its value and change its threshold value to 60%.

b) Select LogPartitionLowWaterMarkExceeded, note its value and change its threshold value to 50%. Polling occurs every 5 minutes, so wait for 5-10 minutes, then verify that the required disk space is available. If you want to free up more disk space in the common partition, change LogPartitionHighWaterMarkExceeded and LogPartitionLowWaterMarkExceeded thread values to lower values (for example, 30% and 20%) again.

After the upgrade finishes, change the threshold fields back their original values. The defaults are 95% for high water mark and 90% for low water mark.