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.

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 1: 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 2: 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

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

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

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

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

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