Changing the IP Address and Hostname for Cisco Unified Communications Manager Release 8.5(1)

Published: December 02, 2010

Revised: July 3, 2012

This document provides the steps to change the IP address or hostname on a Cisco Unified Communications Manager server. You may want to change this IP address for a variety of reasons, which include moving the server from one segment to another or resolving a duplicate IP address problem.

This document contains the following main sections:

Readiness Checklist

Perform the following tasks to ensure that your system is prepared for a successful IP address change.

Note If you have a DNS configured anywhere on the Cisco Unified Communications Manager servers, ensure that the following conditions exist before you change the IP address:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- A forward and reverse lookup zone has been configured.
- The DNS is reachable and working.

Note If you do not receive the results that you expect when you perform these tasks, do not continue with this procedure until you resolve any problems that you find.

Procedure

Step 1 List all servers in the cluster and note whether the nodes are defined by using IP addresses or hostnames.

- From Cisco Unified Communications Manager Administration on the first node, navigate to **System > Server** and click **Find**.

  A list of all servers in the cluster displays.
- Capture this list of servers for later reference.

Step 2 Ensure that you have saved an inventory of both the hostname and IP address of each node in your cluster.

Step 3 Ensure that all servers in the cluster are up and available by checking for any active ServerDown alerts. You can check by using either the Real Time Monitoring Tool (RTMT) or the Command Line Interface (CLI) on the first node.

- To check by using RTMT, access Alert Central and check for ServerDown alerts.
- To check by using the CLI on the first node, enter the following command and inspect the application event log:

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

Step 4 Check the DB replication status on all Cisco Unified Communications Manager nodes in the cluster to ensure that all servers are replicating database changes successfully. You can check by using either RTMT or a CLI command.

- To check by using RTMT, access the Database Summary and inspect the replication status.
- To check by using the CLI, enter the command that the following example shows:

```
admin: show perf query class "Number of Replicates Created and State of Replication"
==>query class :

    - Perf class (Number of Replicates Created and State of Replication)
has instances and values:
    ReplicateCount  -> Number of Replicates Created   = 344
    ReplicateCount  -> Replicate_State                = 2
```

Be aware that the Replicate_State object shows a value of 2 in this case. The following list shows the possible values for Replicate_State:

- 0—Replication Not Started. Either no subscribers exist, or the Database Layer Monitor service has not been running since the subscriber was installed.
- 1—Replicates have been created, but their count is incorrect.
- 2—Replication is good.
- 3—Replication is bad in the cluster.
- 4—Replication setup did not succeed.

Step 5 To check network connectivity and DNS server configuration, enter the CLI command that is shown in the following example:

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

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

Diagnostics Completed
admin:
```

Step 6 Run a manual DRS backup and ensure that all nodes and active services get backed up successfully. For more information, see the *Disaster Recovery System Administration Guide* for your release:

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

Step 7 For security-enabled clusters (Cluster Security Mode 1 - Mixed), update the Certificate Trust List (CTL) file.

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

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

For detailed instructions on updating and managing the CTL file, including adding a new TFTP server to an existing CTL file, see the *Cisco Unified Communications Manager Security Guide*, *Release 8.5(1)*.

You can find this document at the following URL:

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

Initial Trust List and Certificate Regeneration

If you change the IP address or the hostname of a server in a Cisco Unified Communications Manager release 8.0 or later cluster, the Initial Trust List (ITL) file and the certificates in the ITL are regenerated. The regenerated files do not match the files stored on the phones.

Note When you change the host name of a server on a cluster, you must manually delete the ITL file on the phone to enable the phone to accept the new ITL file.

If cluster security is not enabled, perform the steps in the following procedure to reset the phones.

Note If you enable cluster security using Certificate Trust List (CTL) files and USB eTokens, it is not necessary to perform the steps in the following procedure because trust is maintained by the eTokens and the eTokens are not changed.

Single-Server Cluster

If you change the IP address or the hostname of the server in a Cisco Unified Communications Manager release 8.0 or later single-server cluster and you are using ITL files, perform the following steps to reset the phones.

Enable rollback prior to changing the IP address or hostname of the server.

Step 1 Set the enterprise parameter Prepare Cluster for Rollback to pre-8.0 to **True**.

Step 2 Restart TVS and TFTP.

Step 3 Reset all phones. The phones download an ITL file that contains empty TVS and TFTP certificate sections.

Step 4 On the phone, select **Settings > Security > True List > ITL** to verify that the TVS and TFTP certificate sections of the ITL file are empty.

Step 5 Change the IP address or hostname of the server and let the phones configured for rollback register to the cluster.

Step 6 After all the phones have successfully registered to the cluster, set the enterprise parameter Prepare Cluster for Rollback to pre-8.0 to **False**.

Step 7 Restart TVS and TFTP.

Step 8 Reset all phones.

If you use CTL files or tokens, re-run the CTL client after you change the IP address or hostname of the server, or after you change the DNS domain name.

Multi-Server Cluster

In a multi-server cluster, the phones should have primary and secondary TVS servers to validate the regenerated ITL file and certificates. If a phone can not contact the primary TVS server (due to recent configuration changes), it will fall back to the secondary server. The TVS servers are identified by the CM Group assigned to the phone.

In a multi-server cluster, ensure that you change the IP address or hostname on only one server at a time. If you use CTL files or tokens, re-run the CTL client after you change the IP address or hostname of the server, or after you change the DNS domain name.

Changing the Cluster IP Addresses for Servers That IP Addresses Define

This section describes how to change the cluster IP addresses for servers that by IP addresses define. For information about changing cluster IP addresses for servers that hostnames define, see the "Changing the Cluster IP Addresses for Servers That Hostnames Define" section on page 8.

Caution Changing the IP address on any node in a Cisco Unified Communications Manager cluster can interrupt call processing and other system functions. Also, changing the IP address can cause the system to generate certain alarms and alerts, such as ServerDown and SDLLinkOOS, and automatic failover to a backup server may not operate. Because of this potential impact to the system, you must perform IP address changes during a planned maintenance window.

This section contains the following procedures:

Changing the Cluster IP Addresses for Subscriber Servers That IP Addresses Define

Use this procedure to change the IP address of a a subscriber server if your cluster servers are defined by IP address. To successfully change the IP address, you must complete all steps in this procedure.

Note To define subscriber servers on the Cisco Unified Communications Manager publisher server or to determine how a subscriber server is defined, navigate to **System > Server**. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System > Server**.

The Find and List Servers window displays.

Step 2 From the Find and List servers window, choose the subscriber server.

Step 3 Change the IP address of the subscriber server to reflect the new IP address.

Step 4 Ensure that the IP address change is replicated to the subscriber server database by entering the CLI command **`run sql select name,nodeid from ProcessNode`** on all nodes in the cluster. The following example shows the command output:

```
admin: run sql select name,nodeid from ProcessNode
name                nodeid
================== ======
EnterpriseWideData 1
10.3.90.21         4
10.3.90.5          2
```

Step 5 If you are moving the subscriber server to a different subnet that requires a new default gateway address, change the default gateway by using the **set network gateway** CLI command, as the following example shows:

```
admin:set network gateway 10.3.90.2
          ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity

          Do you want to continue ?

Enter "yes" to continue or any other key to abort
yes
executing...
admin:
```

Step 6 Change the IP address of the subscriber server by performing the following tasks:

a. Enter the CLI command **set network ip eth0** *ip_address netmask*

where *ip_address* specifies the new server IP address and *netmask* specifies the new server network mask.

The following output displays:

```
admin: set network ip eth0 10.3.90.21 255.255.254.0
***   W A R N I N G   ***
If there are IP addresses (not hostnames)
configured in CallManager Administration
under System -> Servers
then you must change the IP address there BEFORE
changing it here or call processing will fail.
This will cause the system to restart
======================================================
 Note: To recognize the new IP address all nodes within
       the cluster will have to be manually rebooted.
======================================================
Do you want to continue?
Enter "yes" to continue and restart or any other key to abort
```

b. Enter **yes** and press **Enter**.

Note You can also change the IP address of the default gateway and the subscriber server by using the Cisco Unified Communications Operating System. From Cisco Unified Communications Operating System Administration, choose **Settings > IP > Ethernet**.

Step 7 Reboot all other servers in the cluster, including the publisher node, to update the local name resolution files, such as hosts, rhosts, sqlhosts, and services.

Note These files update only during system startup; you need to restart core network services, such as Cisco DB and Cisco Tomcat, after the files update. Server restart ensures the proper update and service-restart sequence for the IP address changes to take effect.

Note When changing the IP address of more than one subscriber server, perform the following tasks:

- Change the IP address for one server.
- Reboot the cluster.

- Check the replication status.

  If the changed IP address reflects properly, follow the same procedure on the next subscriber server. Otherwise, do not change the IP address of the other servers.

Warning **Avoid making the changes in parallel on several servers at the same time: doing so can lead to .rhosts and sqlhosts files becoming out of sync in the cluster.**

Changing the Cluster IP Address for the Publisher Server That an IP Address Defines

Use this procedure to change the IP address of a a publisher server if your cluster servers are defined by IP address.

Note You cannot use this procedure to change a subscriber host publisher server from one publisher server to another publisher server.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System > Server**.

The Find and List Servers window displays.

Step 2 From the Find and List servers window, choose the publisher server.

Step 3 Change the IP address of the publisher server to reflect the new IP address.

Step 4 Ensure that the IP address change replicates to the subscriber server database by entering the CLI command **`run sql select name,nodeid from ProcessNode`** on all nodes in the cluster. The following example shows the command output:

```
admin: run sql select name,nodeid from ProcessNode
name               nodeid
================== ======
EnterpriseWideData 1
10.3.90.21         4
10.3.90.5          2
```

Step 5 From the Cisco Unified Communications Operating System Administration window of each subscriber server in the cluster, perform the following tasks:

a. Navigate to **Settings > IP > Publisher.**

b. Change the IP address of the publisher server.

Step 6 If you are moving the server to a different subnet that requires a new default gateway address, change the default gateway by using the set network gateway CLI command, as the following example shows:

```
admin:set network gateway 10.3.90.2
          ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity

          Do you want to continue ?
```

```
Enter "yes" to continue or any other key to abort
yes
executing...
admin:
```

Step 7 To change the IP address of the publisher server, perform one of the following tasks:

- To change the IP address from Cisco Unified Communications Operating System Administration
  1. Choose **Settings > IP > Ethernet**.
  2. Enter the new IP addresses.
  3. Click **Save**. The server reboots automatically.
- To change the IP address by using a CLI command
  1. Enter the CLI command **set network ip eth0** *ip_address netmask*

     where *ip_address* specifies the new server IP address and *netmask* specifies the new server network mask.

     The following output displays:

```
admin: set network ip eth0 10.3.90.21 255.255.254.0
***   W A R N I N G   ***
If there are IP addresses (not hostnames)
configured in CallManager Administration
under System -> Servers
then you must change the IP address there BEFORE
changing it here or call processing will fail.
This will cause the system to restart
======================================================
 Note: To recognize the new IP address all nodes within
       the cluster will have to be manually rebooted.
======================================================
Do you want to continue?
Enter "yes" to continue and restart or any other key to abort
```

  2. Enter **yes** and press **Enter**.

Step 8 After the publisher server reboots automatically, reboot all subscriber servers to update the local name resolution files, such as hosts, rhosts, sqlhosts, and services.

Note These files update only during system startup; you need to restart core network services, such as Cisco DB and Cisco Tomcat, after the files update. Server restart ensures the proper update and service-restart sequence for the IP address changes to take effect.

Step 9 Perform a manual DRS backup and ensure that all nodes and active services back up successfully. For more information, see the *Disaster Recovery System Administration Guide* for your release.

Changing the Cluster IP Addresses for Servers That Hostnames Define

This section describes how to change the cluster IP addresses for servers that hostnames define. For information about changing cluster IP addresses for servers that IP addresses define, see the "Changing the Cluster IP Addresses for Servers That IP Addresses Define" section on page 5.

Caution Be aware that a DRS backup that you take from a server with a particular hostname cannot be restored on a server (either a publisher or subscriber node) with a different hostname, even after you reinstall that node.

This section contains the following procedures:

- Changing the Cluster IP Addresses for Subscriber Servers That Hostnames Define, page 9
- Changing the Cluster IP Addresses for Publisher Servers That Hostnames Define, page 11

Changing the Cluster IP Addresses for Subscriber Servers That Hostnames Define

Use this procedure to change the IP address of a a subscriber server if hostnames define your cluster servers.

Procedure

Step 1 Change the DNS record of the subscriber server to point to the new IP address. Ensure that you correctly update both the forward (A) and reverse (PTR) records. You must refresh your DNS cache to ensure that the records update correctly.

Note DNS servers comprise part of the network infrastructure. Cisco Unified Communications Manager servers do not and cannot run DNS services.

Step 2 Verify that the DNS change propagates to other nodes by using the **utils network host** and **show tech network hosts** CLI commands on all cluster nodes:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11

admin:show tech network hosts
 -------------------- show platform network --------------------

 /etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.

127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Step 3 If you are moving the server to a different subnet that requires a new default gateway address, change the default gateway by using the **set network gateway** CLI command, as the following example shows:

```
admin:set network gateway 10.3.90.2
          ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity

          Do you want to continue ?

Enter "yes" to continue or any other key to abort
yes
executing...
admin:
```

Step 4 Change the IP address of the subscriber server by performing the following tasks:

a. Enter the CLI command **set network ip eth0** *ip_address netmask*

where *ip_address* specifies the new server IP address and *netmask* specifies the new server network mask.

The following output displays:

```
admin: set network ip eth0 10.3.90.21 255.255.254.0
***   W A R N I N G   ***
If there are IP addresses (not hostnames)
configured in CallManager Administration
under System -> Servers
then you must change the IP address there BEFORE
changing it here or call processing will fail.
This will cause the system to restart
======================================================
 Note: To recognize the new IP address all nodes within
       the cluster will have to be manually rebooted.
======================================================
Do you want to continue?
Enter "yes" to continue and restart or any other key to abort
```

b. Enter **yes** and press **Enter**.

Note You can also change the IP address of the default gateway and the server by using the Cisco Unified Communications Operating System. From Cisco Unified Communications Operating System Administration, choose **Settings > IP > Ethernet**.

Step 5 Reboot all other servers in the cluster, including the publisher server, to update the local name resolution files, such as hosts, rhosts, sqlhosts, and services.

Note These files update only during system startup; you need to restart core network services, such as Cisco DB and Cisco Tomcat, after the files update. Server restart ensures the proper update and service-restart sequence for the IP address changes to take effect.

Note When changing the IP address of more than one subscriber server, perform the following tasks:

- Change the IP address for one server.
- Reboot the cluster.
- Check the replication status.

If the changed IP address reflects properly, follow the same procedure on the next subscriber server. Otherwise, do not change the IP address of the other servers.

Warning **Avoid making the changes in parallel on several servers at the same time: doing so can lead to .rhosts and sqlhosts files becoming out of sync in the cluster.**

Step 6 Verify that the DNS change propagates to other nodes by using the **utils network host** and **show tech network hosts** CLI commands on all cluster nodes:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11

admin:show tech network hosts
 -------------------- show platform network --------------------

 /etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.

127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Step 7 Perform a manual DRS backup and ensure that all nodes and active services back up successfully. For more information, see the *Disaster Recovery System Administration Guide* for your release.

Changing the Cluster IP Addresses for Publisher Servers That Hostnames Define

Use this procedure to change the IP address of a publisher server if hostnames define your servers.

Procedure

Step 1 Change the DNS record of the publisher server to point to the new IP address. Ensure that you update both the forward (A) and reverse (PTR) records correctly.

Note DNS servers comprise part of the network infrastructure. Cisco Unified Communications Manager servers do not and cannot run DNS services.

Step 2 Verify that the DNS change propagates to other nodes by using the **utils network host** and **show tech network hosts** CLI commands on all cluster nodes:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11

admin:show tech network hosts
 -------------------- show platform network --------------------

 /etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.

127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Step 3 From the Cisco Unified Communications Operating System Administration window (http://*subscriber_ip_address*/cmplatform) of each subscriber server in the cluster, perform the following tasks:

a. Navigate to **Settings > IP > Publisher**.

b. Change the IP address of the publisher server.

Step 4 If you are moving the server to a different subnet that requires a new default gateway address, change the default gateway by using the **set network gateway** CLI command, as the following example shows:

```
admin:set network gateway 10.3.90.2
          ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity

          Do you want to continue ?

Enter "yes" to continue or any other key to abort
yes
executing...
admin:
```

Step 5 Change the IP address of the publisher server by using the CLI by performing the following tasks:

a. Enter the CLI command **set network ip eth0** *ip_address netmask*

where *ip_address* specifies the new server IP address and *netmask* specifies the new server network mask.

The following output displays:

```
admin: set network ip eth0 10.3.90.21 255.255.254.0
***   W A R N I N G   ***
If there are IP addresses (not hostnames)
configured in CallManager Administration
under System -> Servers
then you must change the IP address there BEFORE
```

```
changing it here or call processing will fail.
This will cause the system to restart
======================================================
 Note: To recognize the new IP address all nodes within
       the cluster will have to be manually rebooted.
======================================================
Do you want to continue?
Enter "yes" to continue and restart or any other key to abort
```

b. Enter **Yes** and press **Enter**.

Note You can also change the IP address of the default gateway and the server by using the Cisco Unified Communications Operating System. From Cisco Unified Communications Operating System Administration, choose **Settings > IP > Ethernet**.

Step 6 After the publisher server reboots automatically as a result of the **set network ip** command, reboot all subscriber servers to update the local name resolution files, such as hosts, rhosts, sqlhosts, and services.

Note These files update only during system startup; you need to restart core network services, such as Cisco DB and Cisco Tomcat, after the files update. Server restart ensures the proper update and service-restart sequence for the IP address changes to take effect.

Step 7 Ensure that local resolution of the subscriber node also resolves to the new IP address by running the **utils network host** and **show tech network hosts** CLI commands:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11

admin:show tech network hosts
 -------------------- show platform network --------------------

 /etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.

127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Step 8 From the Cisco Unified Communications Manager Administration window, navigate to **System > Enterprise Parameters**.

Step 9 Under Phone URL Parameters, change all URLs that contain the old IP address to reflect the new IP address.

Step 10 Perform a manual DRS backup and ensure that all nodes and active services back up successfully. For more information, see the *Disaster Recovery System Administration Guide* for your release.

Changing the Hostname for Servers in a Cluster

The section provides procedures for changing the hostname of publisher and subscriber servers.

This section contains the following procedures:

Changing the Hostname of Subscriber Servers

Use the following procedure to change the hostname of subscriber servers in a cluster.

Procedure

Step 1 Change the DNS record of the subscriber server to point to the new IP address. Ensure that forward (A) and reverse (PTR) records update correctly.

Note DNS servers comprise part of the network infrastructure. Cisco Unified Communications Manager servers do not and cannot run DNS services.

Step 2 Perform one of the following tasks:

- If the servers are defined by IP address and you are only changing the server hostname, skip to Step 6.
- If you are changing the IP address or the server is defined by hostname, continue with Step 3.

Step 3 From the Cisco Unified Communications Manager Administration window, perform the following tasks:

a. Navigate to **System > Server**.

b. Change the hostname of the server under Server Configuration.

Step 4 Ensure that the hostname change replicates to all nodes in the cluster by entering the CLI command **`run sql select name,nodeid from ProcessNode`**.

Step 5 Repeat on all nodes in the cluster.

Step 6 Change the hostname of the server by performing one of the following tasks:

- Change the hostname by using a CLI command
  1. Enter the CLI command **`set network hostname`** *hostname*.
  2. Enter **`Yes`** and press **Enter**. This command automatically reboots this server with the new hostname.
- Change the hostname from Cisco Unified Communications Operating System Administration
  1. Navigate to **Settings -> IP -> Ethernet**.
  2. Change IP address and, if necessary, change the default gateway to the new address.

3. Click the **Save** button, which automatically reboots this server with the new changes.

Note Changing the hostname triggers an automatic, self-signed Certificate Regeneration. After the server reboots automatically, secure connections to this server fail until the CTL client runs anew and the CTL file updates.

Step 7 If the IP address changes along with hostname and the server moves to a new subnet, first change the server Default Gateway to the new address by using the **set network gateway** *ipaddress* CLI command.

Note When the default gateway changes prior to the next step, ensure that the server moves to the new subnet and has access to the default gateway prior to the next step. During Cisco Unified Communications Manager server startup, the Verify Network script checks server access to the default gateway. If the server cannot communicate with the default gateway at startup time, the Verify Network script will fail and startup may be delayed. If you are using Manual DHCP configuration and the DHCP server is not reachable or does not give out an IP address to the server, the system will not boot; instead, the system continues to wait at the Verify Network startup phase.

Step 8 Reboot all other servers in the cluster, including the publisher, to update the local name resolution files such as hosts/rhosts/sqlhosts/service.

Note These files update only during system startup; you need to restart core network services, such as Cisco DB and Cisco Tomcat, after the files update. Server restart ensures the proper update and service-restart sequence for the IP address changes to take effect.

Step 9 Verify that the DNS change propagates to other nodes by using the **utils network host** and **show tech network hosts** CLI commands on all cluster nodes:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11

admin:show tech network hosts
 -------------------- show platform network --------------------

 /etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.

127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

You can also use the **utils diagnose module validate_network** command on all cluster nodes. This diagnostics module checks that you configured DNS client services correctly, that the server can connect to the DNS server, and that Forward (A) and Reverse (PTR) records are present and match the server IP address and hostname.

Note Do not proceed until the change propagates to all nodes.

Step 10 From the publisher server, run **utils dbreplication reset all** to set up replication across the whole cluster again.

Changing the Hostname for the Publisher Server

Use the following steps to change the hostname of a publisher server.

Procedure

Step 1 Change the DNS record of the publisher server to the new hostname. If the IP address is going to change at the same time, ensure that the DNS servers also reflect the IP address. Ensure that forward (A) and reverse (PTR) records update correctly.

Note DNS servers constitute part of the network infrastructure. Cisco Unified Communications Manager servers do not and cannot run DNS services.

Note Skip Step 2 through Step 5 if IP addresses define the servers and you are changing only the server hostname.

Step 2 From the Cisco Unified Communications Manager Administration window, perform the following tasks:

a. Navigate to **System > Server**.

b. Under Server Configuration, change the hostname and/or IP address of the server.

Step 3 Ensure that the hostname change replicates to all nodes in the cluster by entering the CLI command **run sql select name, nodeid from ProcessNode**.

Step 4 Repeat on all nodes in the cluster.

Step 5 From the Cisco Unified Communications Operating System Administration window (http://*subscriber_ip_address*/cmplatform or http://*subscriber_ip_address*/iptplatform) of each subscriber server in the cluster, perform the following tasks:

a. Navigate to **Settings > IP > Publisher**.

b. Change the hostname of the publisher server.

Note You can use the following CLI commands to change the IP address and/or hostname of the publisher server on the subscriber servers: **set network cluster publisher ip** or **set network cluster publisher hostname**.

Step 6 On the publisher server, change the hostname of the server by performing the following tasks:

a. Enter the CLI command **`set network hostname`** *hostname*.

b. Enter **`Yes`** and press **Enter**. This action automatically reboots this server with the new hostname.

Note Changing the hostname triggers an automatic, self-signed Certificate Regeneration. After the server reboots automatically, secure connections to this server fail until the CTL client runs anew and the CTL file updates.

Step 7 If the IP address changes along with hostname and the server moves to a new subnet, first change the server Default Gateway to the new address by using the **`set network gateway`** *ip_address* CLI command.

Note When the default gateway changes prior to the next step, ensure that the server moves to the new subnet and has access to the default gateway prior to the next step. During Cisco Unified Communications Manager server startup, the Verify Network script checks server access to the default gateway. If the server cannot communicate with the default gateway at startup time, the Verify Network script will fail and startup may be delayed. If you are using Manual DHCP configuration and the DHCP server is not reachable or does not give out an IP address to the server, the system will not boot; instead, the system continues to wait at the Verify Network startup phase.

Step 8 From the CLI or Cisco Unified Communications Operating System Administration, reboot all other servers in the cluster, including the publisher, to update the local name resolutions files, such as hosts/rhosts/sqlhosts/service. You must reboot the entire cluster after you change each node.

Note These files update only during system startup; you need to restart core network services, such as Cisco DB and Cisco Tomcat, after the files update. Server restart ensures the proper update and service-restart sequence for the IP address changes to take effect.

Step 9 Verify that the DNS change propagates to other nodes by using the **`utils network host`** and **`show tech network hosts`** CLI commands on all cluster nodes:

```
admin:utils network host lg-pub-4
Hostname lg-pub-4 resolves to 14.86.13.11

admin:show tech network hosts
 -------------------- show platform network ---------------------

 /etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.

127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
```

```
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Alternatively, you can use the **utils diagnose module validate_network** command on all cluster nodes. This diagnostics module ensures that, if DNS client services are configured, connectivity to DNS server is present, and Forward (A) and Reverse (PTR) records are present and match the server IP address as well as hostname.

Caution Do not proceed if the new hostname does not resolve to the correct IP address.

Step 10 From the publisher node, run **utils dbreplication reset all** to set up replication across the whole cluster again.

Post-Change Task List

After you finish changing the IP addresses of your cluster, complete the following tasks.

Procedure

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

For detailed instructions on updating and managing the CTL file, including adding a new TFTP server to an existing CTL file, see the *Cisco Unified Communications Manager Security Guide*, *Release 8.5(1)*.

You can find this document at the following URL:

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

Step 2 After you finish updating the CTL file, restart all nodes in the cluster.

Step 3 Ensure that all servers in the cluster are up and available by checking for any active ServerDown alerts. You can check by using either the Real Time Monitoring Tool (RTMT) or the Command Line Interface (CLI) on the first node.

- To check by using RTMT, access Alert Central and check for ServerDown alerts.
- To check by using the CLI on the first node, enter the following command and inspect the application event log:

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

Step 4 Check the DB replication status on all Cisco Unified Communications Manager nodes in the cluster to ensure that all servers are replicating database changes successfully. You can check by using either RTMT or a CLI command.

- To check by using RTMT, access the Database Summary and inspect the replication status.
- To check by using the CLI, enter the command that the following example shows:

```
admin: show perf query class "Number of Replicates Created and State of Replication"
==>query class :

        - Perf class (Number of Replicates Created and State of Replication)
    has instances and values:
        ReplicateCount  -> Number of Replicates Created   = 344
        ReplicateCount  -> Replicate_State               = 2
```

Be aware that the Replicate_State object shows a value of 2 in this case. The following list shows the possible values for Replicate_State:

- 0—Replication Not Started. Either no subscribers exist, or the Database Layer Monitor service has not been running since the subscriber was installed.
- 1—Replicates have been created, but their count is incorrect.
- 2—Replication is good.
- 3—Replication is bad in the cluster.
- 4—Replication setup did not succeed.

Step 5 In Cisco Unified Reporting, generate the Unified CM Database Status report. Look for any errors or warnings in this report.

Step 6 In Cisco Unified Reporting, generate the Unified CM Cluster Overview report. Look for any errors or warnings in this report.

Step 7 Reconfigure the netdump server and clients by using the **`utils netdump`** CLI commands. For more information, see Appendix A in the *Cisco Unified Communications Operating System Administration Guide*.

Step 8 Run a manual DRS backup and ensure that all nodes and active services back up successfully. For more information, see the *Disaster Recovery System Administration Guide* for your release.

Note You must run a manual DRS backup after you change the IP address of a node, because you cannot restore a node with a DRS file that contains a different IP address or hostname. The post-change DRS file will include the new IP address or hostname.

Step 9 Update all relevant IP phone URL parameters.

Step 10 In Cisco Unified Communications Manager Administration under **System > Enterprise Parameters,** update all relevant IP phone services.

Step 11 Update IPSec tunnels that terminate to the Cisco Unified Communications Manager.

Step 12 Update RTMT custom alerts and saved profiles:

- RTMT custom alerts that are derived from performance counters include the hard-coded server IP address. You must delete and reconfigure these custom alerts.
- RTMT saved profiles that have performance counters include the hard-coded server IP address. You must delete and re-add these counters and then save the profile to update it to the new IP address.

Step 13 Update the DHCP server that runs on Cisco Unified Communications Manager.

Step 14 Check and make any required configuration changes to other associated Cisco Unified Communications components, including the following ones:

Note Consult the documentation for your product to determine how to make any required configuration changes.

- Cisco Unity
- Cisco Unity Connection
- Cisco Unity Express
- SIP/H.323 trunks

- IOS Gatekeepers
- Cisco Unified MeetingPlace
- Cisco Unified MeetingPlace Express
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- DHCP Scopes for IP phones
- SFTP servers that are used for Cisco Unified Communications Manager trace collection, CDR export, or as a DRS backup destination
- IOS hardware resources (conference bridge, media termination point, transcoder, RSVP agent) that register with Cisco Unified Communications Manager
- IPVC video MCUs that register or integrate with Cisco Unified Communications Manager
- Cisco Emergency Responder
- Cisco Unified Application Environment
- Cisco Unified Presence
- Cisco Unified Personal Communicator
- Associated routers and gateways

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at

http://www.access.gpo.gov/bis/ear/ear_data.html

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.