IP Address, Domain, Node Name and Hostname for IM and Presence Service on Cisco Unified Communications Manager, Release 9.1(1)

May 14, 2014
IP Address, Domain, Node Name and Hostname for IM and Presence Service on Cisco Unified Communications Manager, Release 9.1(1)

© 2014 Cisco Systems, Inc. All rights reserved.
Readiness Checklist

May 14, 2014

This document provides the steps to change the IP address, hostname or domain of an IM and Presence server. You may want to change these values for a variety of reasons, including moving the server from one domain to another or resolving a duplicate IP address problem.

Warning

You must perform these procedures during a scheduled maintenance window.

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

Caution

If you do not receive the results that you expect when you perform these tasks, do not continue with this procedure until after 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 CM IM and Presence Administration on the first node, navigate to System > Cluster Topology.
- Check the list of available servers in the left frame of the Cluster Topology Details window.
- Capture the list of available servers for later reference.

Step 2

Ensure that you have saved a list of the IP address, hostname and domain for each node in your cluster.

Step 3

Ensure that all servers in the cluster are running and available by checking for any active ServerDown alerts. You can do this by entering the following command on the publisher node:

file search activelog syslog/CiscoSyslog ServerDown

Step 4

Check the DB replication status to ensure that all servers are replicating database changes successfully. Enter the following CLI command on the publisher node:

utils dbreplication runtimestate

Sample output is as follows:

DB and Replication Services: ALL RUNNING

Cluster Replication State: Replication status command started at: 2012-02-26-09-40
Replication status command COMPLETED 269 tables checked out of 269
No Errors or Mismatches found.

Use ‘file view activelog cm/trace/dbl/sdi/ReplicationStatus.2012_02_26_09_40_34.out’
to see the details

DB Version: ccm8_6_3_10000_23
Number of replicated tables: 269

Cluster Detailed View from PUB (2 Servers):

<table>
<thead>
<tr>
<th>SERVER-NAME</th>
<th>IP ADDRESS</th>
<th>PING (msec)</th>
<th>RPC?</th>
<th>REPLICATION STATUS</th>
<th>REPL. QUEUE</th>
<th>REPL. TABLES</th>
<th>LOOP?</th>
<th>DBver&amp;REPL. SETUP</th>
<th>(RTMT) &amp; details</th>
</tr>
</thead>
<tbody>
<tr>
<td>gwydia020218</td>
<td>10.53.46.130</td>
<td>0.038</td>
<td>Yes</td>
<td>Connected</td>
<td>0</td>
<td>match</td>
<td>Yes</td>
<td>(2) PUB Setup Completed</td>
<td></td>
</tr>
<tr>
<td>gwydia020220</td>
<td>10.53.46.133</td>
<td>0.248</td>
<td>Yes</td>
<td>Connected</td>
<td>128</td>
<td>match</td>
<td>Yes</td>
<td>(2) Setup Completed</td>
<td></td>
</tr>
</tbody>
</table>

Note: It is important to verify that REPLICATION SETUP (RTMT) & details all report a state of 2.
Anything other than 2 means that there is a problem with database replication.

Step 5  Check network connectivity and DNS server configuration. To do this, 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  If you are changing the IP address of a server and you use the Domain Name System (DNS) in your
network, ensure the following before you change the IP address:
- There is a forward and reverse lookup zone configured.
- The DNS is reachable and working.

Step 7  Run a manual DRS backup and ensure that all nodes and active services are backed up successfully.

Step 8  Disable High Availability (HA) on any subcluster that contains a node where the IP address, hostname
or domain will be changed. Select System > Cluster Topology in Cisco Unified CM IM and Presence
Administration. For more information on how to disable HA, see Configuration and Administration of
IM and Presence Service on Cisco Unified Communications Manager.

Step 9  For each cluster where the publisher/subscriber node being changed is an intercluster peer, remove the
publisher’s/subscriber’s cluster from the list of intercluster peers.

For example, ClusterA, ClusterB and ClusterC are all intercluster peers. You want to change the
hostname on the publisher node of ClusterA. You must first remove the ClusterA publisher node from
the list of intercluster peers on both ClusterB and ClusterC.

Step 10 Restart the Cisco Intercluster Sync Agent on the publisher and subscriber nodes of the first subcluster in
each cluster.

Step 11 If the notifications in the Cisco Unified CM IM and Presence Administration GUI indicate that a restart
is needed, restart the Cisco XCP Router on all nodes in the clusters.

Step 12 In IM and Presence Release 9.0 and later, the Single Sign-On (SSO) feature is available for
IM and Presence interfaces, including the Real-Time Monitoring Tool (RTMT). The IM and Presence
server hostname is a critical piece of information for SSO to function correctly. Cisco recommends that
you disable SSO prior to changing the IM and Presence server hostname. After you change the hostname, you can re-enable SSO using the new hostname. For more information about SSO, see the “Single Sign-On Configuration” section of Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager.

**Note** Keep in mind that after you disable SSO, you will need to enter login credentials to access IM and Presence. Ensure that you remember your login credentials before disabling SSO, otherwise you may be locked out of IM and Presence applications.

**Step 13** Run the following CLI commands on all nodes in the cluster to stop the following IM and Presence services:

- `utils service stop Cisco Config Agent`
- `utils service stop Cisco Intercluster Sync Agent`
- `utils service stop Cisco Client Profile Agent`
- `utils service stop Cisco Presence Engine`
- `utils service stop Cisco OAM Agent`
- `utils service stop Cisco SIP Proxy`
- `utils service stop Cisco Sync Agent`
- `utils service stop Cisco XCP Router`
- `utils service stop Cisco Presence Datastore`
- `utils service stop Cisco SIP Registration Datastore`
- `utils service stop Cisco Login Datastore`
- `utils service stop Cisco Route Datastore`
- `utils service stop Cisco XCP Config Manager`

**Troubleshooting Tip**
Failure to properly shut down these services prior to changing the IP address or hostname could potentially trigger erroneous alerts and core dumps during the renaming process. If you inadvertently skip this step, and an alarm or core is generated as a result, you must manually clear it and remove the core with the following CLI command: `file delete activelog core`

**Related Documents**
- Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager
- Disaster Recovery System Administration Guide
Modify IP Addresses for Servers Defined by IP Address

This section describes how to change the IP addresses for servers that are defined by IP addresses.

**Caution**
Changing the IP address on any node in a IM and Presence cluster can interrupt presence services and other system functions. Also, changing the IP address can cause the system to generate certain alarms and alerts, such as ServerDown and SDLLinkOSS, 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.

Modify IP Address of Publisher Server Defined by IP Address

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

**Note**
You cannot use this procedure to change a publisher server of the subscriber host to another publisher server.

**Before You Begin**
- See the Readiness Checklist, page 1-1
- Ensure that the IP addresses of subscriber nodes are changed (if required) prior to changing publisher IP address.

**Caution**
If you need to change the gateway address, you must do so before you change the IP address. If you first change the IP address, the IM and Presence server will restart immediately and you will not be able to change the gateway.
Modify IP Addresses for Servers Defined by IP Address

Chapter 2  Modify IP Addresses for Servers Defined by IP Address

Procedure

Step 1  From Cisco Unified CM IM and Presence Administration, perform the following tasks on the publisher server:

a. Navigate to **System > Cluster Topology**.

b. Select the publisher node from the Cluster Topology tree-view.

c. In the Node Configuration section, change the IP address of the IM and Presence server.

d. Select **Save**.

Step 2  From Cisco Unified Communications Manager Administration, perform the following tasks to reflect the new IP address on the publisher server:

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

b. Select **Find** from the Find and List Servers window to display the subscriber server.

c. Verify that the new IP address exists in the application server list.

**Note**  Do not proceed if the new IP address is not among the list of servers.

Step 3  Ensure that the IP address change is replicated to all subscriber nodes in the cluster by entering the following command on each subscriber node:

```sql
run sql select name,nodeid from ProcessNode
```

The following example shows the command output:

```
name               nodeid
================== ======
EnterpriseWideData 1
10.3.90.21         4
10.3.90.5          2
```

**Note**  Do not proceed if the IP address has not been replicated to all nodes in the cluster.

Step 4  Change the IP address of the publisher server on each subscriber server in the cluster by performing the following tasks in the CLI for each subscriber server:

a. Enter the following command:

```
set network cluster publisher ip new_ip_address
```

b. Enter **Yes** and press **Enter**. The server restarts automatically.

Step 5  Change the IP address of the publisher server, and if necessary the default gateway, to the new address by performing the following tasks from the CLI:

a. If you are moving the server to a different subnet that requires a new default gateway address, enter the CLI command **set network gateway**

The following output displays:

```
admin: set network gateway 10.53.56.1
```

**WARNING:** Changing this setting will invalidate software license on this server. The license will have to be re-hosted.
Chapter 2  Modify IP Addresses for Servers Defined by IP Address

Modify IP Address of Publisher Server Defined by IP Address

b. Enter yes and press Enter.

c. To change the IP address of the publisher server, enter the CLI command set network ip eth0
   ip_address netmask gateway

   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 10.53.57.101 255.255.255.224 10.53.57.1

   WARNING: Changing this setting will invalidate software license
   on this server. The license will have to be re-hosted.

Continue (y/n)?

d. Enter yes and press Enter.

Note
If you changed switches in addition to changing the gateway and IP address for the IM and Presence
server, complete the following steps while the server is automatically restarting. Otherwise, some of the
IM and Presence scripts may fail network connectivity checks upon startup.

• watch the restart screen
• enter a ping –t on the old IP address
• when the pings are no longer successful, disconnect from the old switch and connect to the new
  switch

Step 6  After the publisher node has restarted, restart all subscriber nodes with the following CLI command:
utils system restart

Step 7  After all nodes have restarted successfully, run the following CLI command on the publisher node to
reset replication:
utils dbreplication reset all

Note  This command may take up to 15 minutes to complete.

Step 8  After the utils dbreplication reset all command is complete, restart the publisher node with the
following CLI command:
utils system restart

Step 9  After the publisher node has restarted, restart all the subscriber nodes in the cluster with the following
CLI command:
utils system restart
Note
When changing the IP address of more than one server in a cluster, 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 server. Otherwise, do not change the IP address of the other servers.

Related Topics
- Disaster Recovery System Guide
- Cisco Unified Communications Operating System Administration Guide

What To Do Next
Post-Change Task List, page 7-1

Modify IP Address of Subscriber Server Defined by IP Address

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

When changing the IP address of more than one subscriber server, we recommend that you:

a. Change the IP address for one server at a time.

b. Restart all other servers in the cluster (including the publisher server) to update the local name resolution files including database related configuration files.

Caution
Caution! Do not change the IP address of more than one server at the same time because it can cause local name resolution files to be out of sync in the cluster.

Before You Begin
Post-Change Task List, page 7-1

Caution
If you need to change the gateway address, you must do so before you change the IP address. If you change the IP address first, the IM and Presence server will restart immediately and you will not be able to change the gateway.

Procedure

Step 1
From Cisco Unified CM IM and Presence Administration, perform the following tasks on the subscriber server:


b. Select the publisher node from the Cluster Topology tree-view.

c. In the Node Configuration section, change the IP address of the IM and Presence server.
d. Select Save.

**Step 2**

From Cisco Unified Communications Manager Administration, perform the following tasks to reflect the new IP address on the subscriber server:

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

b. Select **Find** from the Find and List Servers window to display the subscriber server.

c. Verify that the new IP address exists in the application server list.

**Note**
Do not proceed if the new IP address is not among the list of servers.

**Step 3**

Ensure that the IP address change is replicated to all the nodes in the cluster by entering the following CLI command:

```sql
run sql select name,nodeid from ProcessNode
```

The following example shows the command output:

<table>
<thead>
<tr>
<th>name</th>
<th>nodeid</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnterpriseWideData</td>
<td>1</td>
</tr>
<tr>
<td>10.3.90.21</td>
<td>4</td>
</tr>
<tr>
<td>10.3.90.5</td>
<td>2</td>
</tr>
</tbody>
</table>

**Note**
Do not proceed if the IP address has not been replicated to all nodes in the cluster.

**Step 4**

Repeat Steps 1 to 3 on all subscriber nodes in the cluster, as required.

**Step 5**

Change the IP address of the subscriber server, and if necessary the default gateway, to the new address by performing the following tasks:

a. If you are moving the server to a different subnet that requires a new default gateway address, enter the CLI command **set network gateway**

The following output displays:

```
admin:set network gateway 10.53.56.2
WARNING: Changing this setting will invalidate software license on this server. The license will have to be re-hosted.
```

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

b. To change the IP address of the subscriber server, enter the CLI command **set network ip eth0 ip_address netmask gateway**

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 10.53.57.101 255.255.255.224 10.53.57.1
WARNING: Changing this setting will invalidate software license on this server. The license will have to be re-hosted.
```

Continue (y/n)?
d. Enter `yes` and press `Enter`.

**Troubleshooting Tip**
If you changed switches in addition to changing the gateway and IP address for the IM and Presence server, complete these steps while the server is automatically restarting. Otherwise, some of the IM and Presence scripts may fail network connectivity checks upon startup.

- watch the restart screen
- enter a `ping –t` on the old IP address
- when the pings are no longer successful, disconnect from the old switch and connect to the new switch

**Related Topics**
- *Disaster Recovery System Guide*
- *Cisco Unified Communications Operating System Administration Guide*

**What To Do Next**
Post-Change Task List, page 7-1
Modify IP Addresses for Servers Defined by Hostname/FQDN

May 14, 2014

- Modify IP Address of Publisher Server Defined by Hostname/FQDN, page 3-1
- Modify IP Address of Subscriber Server Defined by Hostname/FQDN, page 3-4

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

Modify IP Address of Publisher Server Defined by Hostname/FQDN

Use this procedure to change the IP address of a publisher server if your servers are defined by hostname or FQDN. DNS servers comprise part of the network infrastructure. IM and Presence servers do not and cannot run DNS services.

Note
You cannot use this procedure to change a publisher server of the subscriber host to another publisher server.

Before you begin
Readiness Checklist, page 1-1

Procedure

Step 1
Perform the following actions:

a. Change the DNS record of the publisher server to point to the new IP address.

b. Ensure that you correctly update both the forward (A) and reverse (PTR) records.

Step 2
Change the IP address of the publisher server on each subscriber server in the cluster by performing the following tasks in the CLI for each subscriber server:

a. Enter the following command:
Chapter 3      Modify IP Addresses for Servers Defined by Hostname/FQDN

Modify IP Address of Publisher Server Defined by Hostname/FQDN

Step 3

Change the IP address of the publisher server, and if necessary the default gateway, to the new address by performing the following tasks:

a. If you are moving the server to a different subnet that requires a new default gateway address, enter the CLI command `set network gateway`

The following output displays:

```
admin:set network gateway 10.53.56.1
```

WARNING: Changing this setting will invalidate software license on this server. The license will have to be re-hosted.

Continue (y/n)?

b. Enter yes and press Enter.

c. To change the IP address of the publisher server, enter the CLI command `set network ip eth0`

```
set network ip eth0 ip_address netmask gateway
```

where `ip_address` specifies the new server IP address, `netmask` specifies the new server network mask and `gateway` specifies the gateway.

The following output displays:

```
admin:set network ip eth0 10.53.57.101 255.255.255.224 10.53.57.1
```

WARNING: Changing this setting will invalidate software license on this server. The license will have to be re-hosted.

Continue (y/n)?

d. Enter yes and press Enter.

Step 4

After the publisher server restarts automatically, restart all subscriber servers to update the local name resolution files including database related configuration files, and services.

Step 5

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:

Note
If you changed switches in addition to changing the gateway and IP address for the IM and Presence server, complete the following steps while the server is automatically restarting. Otherwise, some of the IM and Presence scripts may fail network connectivity checks upon startup.

- watch the restart screen
- enter a ping -t on the old IP address
- when the pings are no longer successful, disconnect from the old switch and connect to the new switch

Step 6
After the publisher node has restarted, restart all subscriber nodes with the following CLI command:

`utils system restart`

Step 7
After all nodes have restarted successfully, run the following CLI command on the publisher node to check replication:

`utils dbreplication runtimestate`

Note
Depending on the size of the database, it may take several minutes to over an hour for replication to be re-established.

Sample output is as follows:

DDB and Replication Services: ALL RUNNING

DB CLI Status: No other dbreplication CLI is running...

Cluster Replication State: BROADCAST SYNC Completed on 1 servers at: 2012-09-26-15-18
Last Sync Result: SYNC COMPLETED 257 tables sync'ed out of 257
Sync Errors: NO ERRORS

DB Version: ccm9_0_1_10000_9000
Number of replicated tables: 257
Repltimeout set to: 300s

Cluster Detailed View from gwydlvm020105 (2 Servers):

<table>
<thead>
<tr>
<th>SERVER-NAME</th>
<th>IP ADDRESS</th>
<th>PING (msec)</th>
<th>RPC?</th>
<th>REPLICATION STATUS</th>
<th>REPL. QUEUE</th>
<th>DBver</th>
<th>REPL. TABLES</th>
<th>REPL. LOOP?</th>
<th>REPLICA SETUP (RTMT) &amp; details</th>
</tr>
</thead>
<tbody>
<tr>
<td>gwydlvm020105</td>
<td>192.168.20.244</td>
<td>0.038</td>
<td>Yes</td>
<td>Connected</td>
<td>0</td>
<td>match Yes</td>
<td>128</td>
<td>Yes</td>
<td>(2) PUB Setup Completed</td>
</tr>
<tr>
<td>gwydlvm020105</td>
<td>192.168.10.201</td>
<td>0.248</td>
<td>Yes</td>
<td>Connected</td>
<td>128</td>
<td>match Yes</td>
<td>(2) Setup Completed</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note
It is important to verify that REPLICA SETUP (RTMT) & details all report a state of 2. Anything other than 2 means that there is a problem with database replication and that you need to reset replication. Refer to Reset Replication, page 3-4 for more information.
Note

When changing the IP address of more than one server in a cluster, 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 server. Otherwise, do not change the IP address of the other servers.

Reset Replication

If replication does not complete successfully, complete the following steps:

Step 1

Run the following CLI command on the publisher node to reset replication:

```bash
utils dbreplication reset all
```

**Note**

This command may take up to 15 minutes to complete.

Step 2

After the `utils dbreplication reset all` command is complete, restart the publisher node with the following CLI command:

```bash
utils system restart
```

Step 3

After the publisher node has restarted, restart all the subscriber nodes in the cluster with the following CLI command:

```bash
utils system restart
```

Related Topics

- *Disaster Recovery System Guide*
- *Cisco Unified Communications Operating System Administration Guide*

What To Do Next

*Post-Change Task List, page 7-1*

Modify IP Address of Subscriber Server Defined by Hostname/FQDN

Use this procedure to change the IP address of a subscriber server if your servers are defined by hostname or FQDN. DNS servers comprise part of the network infrastructure. IM and Presence servers do not and cannot run DNS services.
When changing IP address of more than one subscriber server, we recommend that you:

a. Change the IP address for one server at a time.
b. Restart all other servers in the cluster (including the publisher server) to update local name resolution files including database related configuration files.

⚠️ Caution
Do not change the IP address of more than one server at the same time because it can cause local name resolution files to be out of sync in the cluster.

**Before you begin**
Readiness Checklist, page 1-1

**Procedure**

**Step 1**
Perform the following actions:

a. Change the DNS record of the subscriber server to point to the new IP address.
b. Ensure that you correctly update both the forward (A) and reverse (PTR) records.
c. Refresh your DNS cache to ensure that the records are correctly updated.

**Step 2**
Change the IP address of the subscriber server, and if necessary the default gateway, to the new address by performing the following tasks:

a. If you are moving the server to a different subnet that requires a new default gateway address, enter the CLI command `set network gateway`

The following output displays:

```
admin: set network gateway 10.3.90.2
*** WARNING ***
This will cause the system to temporarily lose network connectivity
```

Enter "yes" to continue or any other key to abort

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

c. To change the IP address of the subscriber server, enter the CLI command `set network ip eth0 ip_address netmask gateway`

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 10.53.57.101 255.255.255.224 10.53.57.1
*** WARNING ***
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
```

d. Enter `yes` and press **Enter**.
Modify IP Address of Subscriber Server Defined by Hostname/FQDN

Step 3  Verify that the DNS change propagates to other nodes by using the `utils network host` and `show tech network hosts` CLI commands on all the 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 4  Restart all other servers in the cluster (including the publisher server) to update the local name resolution files including database related configuration files.

Troubleshooting Tip
If you changed switches in addition to changing the gateway and IP address for the IM and Presence server, complete these steps while the server is automatically restarting. Otherwise, some of the IM and Presence scripts may fail network connectivity checks upon startup.

- watch the restart screen
- enter a `ping –t` on the old IP address
- when the pings are no longer successful, disconnect from the old switch and connect to the new switch

Related Topics
- Disaster Recovery System Guide
- Cisco Unified Communications Operating System Administration Guide

What To Do Next
Post-Change Task List, page 7-1
Modify Server Hostname

May 14, 2014

- Modify Publisher Server Hostname, page 4-1
- Modify Subscriber Server Hostname, page 4-3

Modify Publisher Server Hostname

Use the following procedure to change the hostname of publisher servers in a cluster. DNS servers comprise part of the network infrastructure. IM and Presence servers do not and cannot run DNS services.

**Before You Begin**
Read the Readiness Checklist, page 1-1.

**Procedure**

**Step 1**
Perform the following actions:

a. Change the DNS record of the publisher server to point to the new hostname, for example, `newhost1` (For illustration purposes, `newhost1` is used in the CLI command examples in this procedure.)

b. Ensure that you correctly update both the forward (A) and reverse (PTR) records.

**Step 2**
Verify that the DNS change propagates to other nodes by running the following CLI command on all the cluster nodes:

```
utils network host newhost1
```

where `newhost1` is the new hostname

The output of this command is as follows:

```
admin:utils network host newhost1
Hostname newhost1 resolves to 14.86.13.11
```

**Step 3**
From Cisco Unified CM IM and Presence Administration, perform the following tasks on the publisher server:


b. Select the publisher node from the Cluster Topology tree-view.
c. In the Node Configuration section, update the Name to reflect the new hostname as follows:
   - If the server is defined by hostname, replace the old hostname with the new hostname. For example, update the Name from “old-host” to “new-host”.
   - If the server is defined by FQDN, update the FQDN value to reference the new hostname rather than the old hostname. For example, update the Name from “old-host.example.com” to “new-host.example.com”.

d. Select Save.

Step 4 From Cisco Unified Communications Manager Administration, perform the following tasks:
   a. Navigate to System > Application Server.
   b. Select Find from the Find and List Servers window to display the server.
   c. Verify that the new node name value is listed among the servers.

   Note: Do not proceed if the new node name value is not among the list of servers.

Step 5 Ensure that the hostname change is replicated to all the nodes in the cluster. To do this, enter the following command from the CLI on all nodes in the cluster:

   run sql select name,nodeid from ProcessNode

   Note: Do not proceed if the updated node name value has not been replicated to all nodes in the cluster.

Step 6 Change the hostname of the publisher server on each subscriber server in the cluster by entering the following command in the CLI for each subscriber server:

   set network cluster publisher hostname <new_hostname>

   For example:

   set network cluster publisher hostname newhost1

Step 7 On the publisher server, change the hostname of the server as follows:
   a. Enter the CLI command set network hostname newhost1
      where newhost1 is the new hostname
   b. Enter Yes and press Enter. This will automatically restart this server with the new hostname.

   Note: Changing the hostname triggers an automatic, self-signed Certificate Regeneration. After the server restarts automatically, secure connections to this server will fail until the CTL client is rerun and the CTL file is updated.

Step 8 After the publisher node has restarted, restart all subscriber nodes with the following CLI command:

   utils system restart

Step 9 After all nodes have restarted successfully, run the following CLI command on the publisher node to reset replication:

   utils dbreplication reset all
Modify Subscriber Server Hostname

Use the following procedure to change the hostname of subscriber servers in a cluster. DNS servers comprise part of the network infrastructure. IM and Presence servers do not and cannot run DNS services.

Before You Begin
Read the Readiness Checklist, page 1-1.

Procedure

Step 1 Perform the following actions:
   a. Change the DNS record of the subscriber server to point to the new hostname, for example, newhost1 (For illustration purposes, newhost1 is used in the CLI command examples in this procedure.)
   b. Ensure that you correctly update both the forward (A) and reverse (PTR) records.

Step 2 Verify that the DNS change propagates to other nodes by running the following CLI command on all the cluster nodes:

   `utils network host newhost1`

   where newhost1 is the new hostname

   The output of this command is as follows:

   `admin:utils network host newhost1
   Hostname newhost1 resolves to 14.86.13.11`
Step 3  From Cisco Unified CM IM and Presence Administration, perform the following tasks on the publisher server:

a. Navigate to **System > Cluster Topology**.

b. Select the subscriber node from the Cluster Topology tree-view.

c. In the Node Configuration section, update the **Name** to reflect the new hostname as follows:

   - If the server is defined by hostname, replace the old hostname with the new hostname. For example, update the **Name** from “old-host” to “new-host”.

   - If the server is defined by FQDN, update the FQDN value to reference the new hostname rather than the old hostname. For example, update the **Name** from “old-host.example.com” to “new-host.example.com”.

d. Select **Save**.

Step 4  From Cisco Unified Communications Manager Administration, perform the following tasks:

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

b. Select **Find** from the Find and List Servers window to display the server.

c. Verify that the new node name value is listed among the servers.

   **Note**  Do not proceed if the new node name value is not among the list of servers.

Step 5  Ensure that the hostname change is replicated to all the nodes in the cluster. To do this, enter the following command from the CLI on all nodes in the cluster:

```
run sql select name,nodeid from ProcessNode
```

   **Note**  Do not proceed if the update node name value has not been replicated to all nodes in the cluster.

Step 6  On the subscriber server, change the hostname of the server as follows:

a. Enter the CLI command `set network hostname newhost1`

   where `newhost1` is the new hostname

b. Enter **Yes** and press **Enter**. This will automatically restart this server with the new hostname.

   **Note**  Changing the hostname triggers an automatic, self-signed Certificate Regeneration. After the server restarts automatically, secure connections to this server will fail until the CTL client is rerun and the CTL file is updated.

Step 7  Restart the publisher node in the cluster with the following command:

```
utils system restart
```

Step 8  Restart all other subscriber nodes in the cluster with the following command:

```
utils system restart
```

Step 9  After all nodes have restarted successfully, run the following CLI command on the publisher node to reset replication:

```
utils dbreplication reset all
```
Note

This command may take up to 15 minutes to complete.

Step 10

After the `utils dbreplication reset all` command is complete, restart the publisher node with the following CLI command:

```
utils system restart
```

Step 11

After the publisher node has restarted, restart all the subscriber nodes in the cluster with the following CLI command:

```
utils system restart
```

Related Topics

- *Cisco Unified Serviceability Administration Guide*
- *Cisco Unified Communications Operating System Administration Guide*
- *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*

What To Do Next

*Post-Change Task List, page 7-1*
CHAPTER 5

Modify Node Name

- Procedure Overview, page 5-1
- Procedure Workflow, page 5-2
- Update IM and Presence Node Name, page 5-2
- Verify Database Replication, page 5-3
- Verify Updates on Cisco Unified Communications Manager, page 5-6

Procedure Overview

This procedure allows you to modify the node name that is associated with an IM and Presence node or group of nodes. This procedure modifies the node name as it appears in the Cluster Topology window in the IM and Presence Administration GUI.

⚠️ Caution

This procedure is used only when changing the node name of an IM and Presence node where there are no network level changes required. If changes to the network IP address, hostname or domain name are required, complete the relevant procedure in this document instead.

⚠️ Caution

Changing the node name on any node in an IM and Presence cluster will result in server restarts and interruptions to presence services and other system functions. Because of this impact to the system, you must perform this node name change procedure during a scheduled maintenance window.

This procedure supports the following node name change scenarios:

- IP address to hostname
- IP address to Fully Qualified Domain Name (FQDN)
- hostname to IP address
- hostname to FQDN
- FQDN to hostname
- FQDN to IP address
Procedure Workflow

The following table contains the step-by-step instructions for modifying the node name that is associated with an IM and Presence node or group of nodes. The detailed instructions for this procedure specify the exact order of steps for performing the change.

If you are performing this procedure across multiple clusters you must complete the changes sequentially on one cluster at a time.

Table 5-1  Workflow to modify the node name

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
</table>
| 1    | Complete the Readiness Checklist on all nodes that are to be updated.  
- This procedure includes several prerequisite steps, including a list of services to shut down prior to making the change.  
- Some of these steps may apply only to the publisher node and therefore you can skip them when you run through the procedure for subscriber nodes. |
| 2    | Update IM and Presence Node Name from the Cisco Unified CM IM and Presence Administration GUI. |
| 3    | Verify Database Replication from the Administration CLI.  
After the node name updates are complete, you must verify database replication. |
| 4    | Verify Updates on Cisco Unified Communications Manager.  
You must ensure that the Application Server entries for the servers that have been updated reflect the new node name on the Cisco Unified Communications Manager Administration GUI. |
| 5    | Complete the Post-Change Task List on the updated node.  
Perform a series of steps to ensure the node is operational again. |

Update IM and Presence Node Name

If multiple servers within a cluster are being modified, you must complete the following procedure sequentially for each of these servers.

If the publisher node is being modified, you must complete this procedure for the subscriber nodes first, before completing the procedure on the publisher node.

Before You Begin

Complete the pre-change tasks. See Readiness Checklist, page 1-1.
**Procedure**

**Step 1** Sign in to the Cisco Unified CM IM and Presence Administration GUI on the server.

**Step 2** Navigate to System > Cluster Topology.

**Step 3** Choose the server from the tree-view on the left hand pane of the Cluster Topology page. On the right hand pane, you should see the Node Configuration section and the Fully Qualified Domain Name/IP Address field.

**Step 4** Update the Fully Qualified Domain Name/IP Address field with the new node name.

**Step 5** Select Save.

**Step 6** If multiple servers within a cluster are being modified, repeat this procedure for each server.

**What To Do Next**

Verify Database Replication, page 5-3.

## Verify Database Replication

You must verify that the new node name has replicated across the cluster.

**Before You Begin**

Update the IM and Presence node name. See Update IM and Presence Node Name, page 5-2.

**Note**

Use the validation mechanisms listed below to verify that the new node name(s) have been replicated across the cluster and that database replication is operational.

**Procedure**

**Step 1** To validate that the new node name has been correctly replicated, run the following command from the Administration CLI on all nodes in the cluster:

```
run sql name from ProcessNode
```

The following example shows the command output:

```
admin:run sql select name from ProcessNode
name
===================== EnterpriseWideData
server1.example.com
server2.example.com
server3.example.com
server4.example.com
```

Verify that there is an entry for each node in the cluster that specifies the new node name. No old node name should appear in the output. Proceed as follows:

- a. If any new node names are missing or if there are references to old node names proceed to Step 2 to further validate database replication.
b. If the output is as expected, the validation has passed and you can ignore the remaining steps in this procedure.

**Step 2**

If the new node name is not correctly listed in Step 1, verify that database replication is in a correct state in the cluster by running the following command from the Administration CLI on the publisher node:

```bash
utils dbreplication runtimestate
```

The following example output displays:

```
admin: utils dbreplication runtimestate

DDB and Replication Services: ALL RUNNING

DB CLI Status: No other dbreplication CLI is running...

Cluster Replication State: BROADCAST SYNC Completed on 1 servers at: 2012-09-26-15-18

Last Sync Result: SYNC COMPLETED 257 tables sync'ed out of 257

Sync Errors: NO ERRORS

DB Version: ccm9_0_1_10000_9000

Number of replicated tables: 257

Repltimeout set to: 300s

Cluster Detailed View from gwydlvm020105 (2 Servers):
```

Proceed as follows:

a. Verify that the output shows a replication status of **Connected** and a replication setup value of **(2) Setup Complete** for each node. This means that the replication network within the cluster is up and you can proceed to Step 3 to repair any mismatches between nodes in the cluster.

b. If the replication status and replication setup value are not as expected, then the replication network within the cluster is broken and you must proceed to Step 5 to attempt to reestablish replication.

**Step 3**

Run the following command from the Administration CLI on the publisher node to attempt to repair replication:

```bash
utils dbreplication repair all
```

The following example shows the command output.

```
admin:utils dbreplication repair all

Replication Repair is now running in the background.
Use command 'utils dbreplication runtimestate' to check its progress

Output will be in file cm/trace/dbl/sdi/ReplicationRepair.2013_03_06_12_33_57.out

Please use "file view activelog cm/trace/dbl/sdi/ReplicationRepair.2013_03_06_12_33_57.out" command to see the output
```

**Note** Depending on the size of the database, it may take several minutes to repair database replication.

Proceed to Step 4 to monitor the progress of the replication repair.
Step 4  Run the following command from the Administration CLI on the publisher node to check the progress of replication repair:

```
utils dbreplication runtimestate
```

The following example shows the output when replication is complete. The text in bold highlights the final status of the replication repair:

```
admin:utils dbreplication runtimestate

DB and Replication Services: ALL RUNNING

Cluster Replication State: Replication repair command started at: 2013-03-06-12-33
Replication repair command COMPLETED 269 tables processed out of 269
No Errors or Mismatches found.

Use 'file view activelog cm/trace/dbl/sdi/ReplicationRepair.2013_03_06_12_33_57.out' to see the details

DB Version: ccm8_6_4_98000_192
Number of replicated tables: 269

Cluster Detailed View from PUB (2 Servers):

<table>
<thead>
<tr>
<th>PING</th>
<th>REPLICA\nIONREPL.DBo\nver&amp; REPL.REPLIC\nATION SETUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>server1</td>
<td>10.53.56.170.052YesConnected0 match Yes (2) PUB Setup Completed</td>
</tr>
<tr>
<td>server2</td>
<td>10.53.56.140.166YesConnected0 match Yes (2) Setup Completed</td>
</tr>
</tbody>
</table>
```

Proceed as follows:

a. If replication repair runs to completion without any errors or mismatches, return to Step 1 to validate that the new node name is now correctly replicated.

b. If errors or mismatches are found, there may be a transient mismatch between servers. Return to Step 3 to run the replication repair again.

Note  If, after several attempts to repair replication, mismatches or errors are being reported, contact your Cisco Support Representative to resolve this issue.

Step 5  Run the following command from the Administration CLI on the publisher node to attempt to reestablish replication:

```
utils dbreplication reset all
```

The following example shows the command output:

```
admin:utils dbreplication reset all
This command will try to start Replication reset and will return in 1-2 minutes. Background repair of replication will continue after that for 1 hour.
Please watch RTMT replication state. It should go from 0 to 2. When all subs have an RTMT Replicate State of 2, replication is complete.
If Sub replication state becomes 4 or 1, there is an error in replication setup.
Monitor the RTMT counters on all subs to determine when replication is complete.
Error details if found will be listed below OK [10.53.56.14]
```

Note  Depending on the size of the database, it may take several minutes to over an hour for replication to be fully reestablished.
Proceed to Step 6 to monitor the progress of the replication reestablishment.

**Step 6**

Monitor the progress of the attempt to reestablish database replication in Step 5 by running the following command from the Administration CLI on the publisher node:

```
utils dbreplication runtimestate
```

The following example output displays:

```
admin: utils dbreplication runtimestate

DDB and Replication Services: ALL RUNNING

DB CLI Status: No other dbreplication CLI is running...

Cluster Replication State: BROADCAST SYNC Completed on 1 servers at: 2012-09-26-15-18
   Last Sync Result: SYNC COMPLETED 257 tables sync'ed out of 257
   Sync Errors: NO ERRORS

DB Version: ccm9_0_1_10000_9000
Number of replicated tables: 257
Repltimeout set to: 300s

Cluster Detailed View from gwydlvm020105 (2 Servers):

<table>
<thead>
<tr>
<th>SERVER-NAME</th>
<th>IP ADDRESS</th>
<th>PING (msec)</th>
<th>REPLICATION RPC?</th>
<th>REPL. STATUS</th>
<th>REPL. QUEUE</th>
<th>REPLICATION SETUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>server1</td>
<td>192.168.10.201</td>
<td>0.038</td>
<td>Yes</td>
<td>Connected</td>
<td>0</td>
<td>match</td>
</tr>
<tr>
<td>server2</td>
<td>192.168.10.202</td>
<td>0.248</td>
<td>Yes</td>
<td>Connected</td>
<td>0</td>
<td>match</td>
</tr>
<tr>
<td>server3</td>
<td>192.168.10.203</td>
<td>0.248</td>
<td>Yes</td>
<td>Connected</td>
<td>0</td>
<td>match</td>
</tr>
<tr>
<td>server4</td>
<td>192.168.10.204</td>
<td>0.248</td>
<td>Yes</td>
<td>Connected</td>
<td>0</td>
<td>match</td>
</tr>
</tbody>
</table>

Replication is considered to be reestablished when all nodes show a replication status of **Connected** and a replication setup value of **(2) Setup Complete**. Proceed as follows:

a. If replication is reestablished, return to Step 1 to validate that the new node name is now correctly replicated.

b. If replication does not recover, contact your Cisco Support Representative to resolve this issue.

---

**Caution**

Do not proceed beyond this point if database replication is broken.

---

**What To Do Next**

Verify Updates on Cisco Unified Communications Manager, page 5-6

---

**Verify Updates on Cisco Unified Communications Manager**

Verify that the Application Server entry for this server has been updated to reflect the new node name on the Cisco Unified Communications Manager Administration GUI.

You must complete this procedure for each node name that has been changed.

**Before You Begin**

Ensure that database replication is operational on all nodes. See Verify Database Replication, page 5-3.
Procedure

Step 1  Sign in to the Cisco Unified Communications Manager Administration GUI and Navigate to System > Application Server.

Step 2  Click Find, if required, on the Find and List Application Servers page.

Step 3  Ensure that an entry exists for the updated node name in the list of Application Servers. If there is no entry, add an entry for the new node name.

What To Do Next

Complete the post-change task list on all applicable nodes within the cluster. See Post-Change Task List, page 7-1.
CHAPTER 6

Modify Server Domain

May 14, 2014

- Procedure Overview, page 6-1
- Procedure Workflow, page 6-2
- Update DNS Records, page 6-3
- Update IM and Presence Node Name, page 6-5
- Update DNS Domain, page 6-6
- Reboot all Servers in Cluster after Domain Update, page 6-8
- Restart Database Replication, page 6-9
- Regenerate Security Certificates, page 6-11

Procedure Overview

This procedure allows an administrator to modify the DNS domain associated with an IM and Presence server or group of servers.

Caution

Changing the domain on any server in an IM and Presence cluster will result in server restarts and interruptions to presence services and other system functions. Because of this impact to the system, you must perform this domain change procedure during a scheduled maintenance window.

While this procedure modifies the DNS domain of the server, it does not attempt to modify the enterprise-wide presence domain, as configured on the Cluster Topology settings of the Cisco Unified CM IM and Presence Administration GUI.

- The enterprise-wide presence domain does not need to align with the DNS domain of any IM and Presence server.
- If you wish to modify the enterprise-wide presence domain for your deployment, see Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager.

Note

- This procedure results in all third party signed security certificates being automatically overwritten with new self-signed certificates. If you wish to have those certificates re-signed by your third party Certificate Authority, you must manually request and upload the new certificate(s).
• Service restarts may be required to pick up these new certificates. Depending on the time required to request new certificates, a separate maintenance window may be required to schedule the service restarts.

• These new certificates cannot be requested in advance of this procedure. Certificate Signing Requests (CSRs) can only be generated after the domain has been changed on the server and the server has been rebooted.

---

**Procedure Workflow**

The following table contains the step-by-step instructions for modifying the DNS domain associated with an IM and Presence server or group of servers. The detailed instructions for this procedure specify the exact order of steps for performing the change on multiple nodes within the cluster.

If you are performing this procedure across multiple clusters you must complete the changes sequentially on one cluster at a time.

**Note**

You must complete each task in this procedure in the exact order presented in this workflow.

Table legend:

- X—step is mandatory
- NA—step does not apply

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Node Name Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Complete the <strong>Readiness Checklist</strong> on all applicable nodes within the cluster.</td>
<td><strong>X</strong></td>
</tr>
<tr>
<td></td>
<td>• This checklist includes a number of prerequisite steps, including a list of services to shut down prior to making the change.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Some of these steps may only be applicable to the publisher node and therefore can be skipped when running through the checklist for subscriber node(s).</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><strong>Update DNS Records</strong> for the server on all applicable nodes within the cluster.</td>
<td><strong>X</strong></td>
</tr>
<tr>
<td></td>
<td>• Update SRV, Forward (A) and Reverse (PTR) records as appropriate to incorporate the new server domain.</td>
<td></td>
</tr>
</tbody>
</table>
Because the DNS domain for the server is being modified, any existing DNS records associated with that server must be updated. This includes the following types of records:

- A Records
- PTR Records
- SRV Records
If multiple servers within a cluster are being modified, you must complete the following procedure for each of these servers.

If the publisher node is being modified, you must complete this procedure on the publisher node first before repeating on any applicable subscriber nodes.

**Note**

- These DNS records must be updated during the same maintenance window as the DNS domain change itself on the server.
- Updating the DNS records before the scheduled maintenance window may adversely affect IM and Presence Service functionality.

**Before You Begin**

Ensure that you have completed the Readiness Checklist. See Readiness Checklist, page 1-1 for more information.

**Procedure**

**Step 1** Remove the old DNS forward (A) record for the server from the old domain.

**Step 2** Create a new DNS forward (A) record for the server within the new domain.

**Step 3** Update the DNS reverse (PTR) record for the server to point to the updated Fully Qualified Domain Name (FQDN) of the server.

**Step 4** Update any DNS SRV records that point to the server.

**Step 5** Update any other DNS records that point to the server.

**Step 6** Verify that all the above DNS changes have propagated to all other nodes within the cluster by running the following commands on the Administration CLI of each node:

- **To validate the new A record:**
  ```
  utils network host new-fqdn
  
  where new-fqdn is the updated FQDN of the server.
  
  For example:
  ```
  ```
  admin: utils network host server1.new-domain.com
  Local Resolution:
  server1.new-domain.com resolves locally to 10.53.50.219
  
  External Resolution:
  server1.new-domain.com has address 10.53.50.219
  ```

- **To validate the updated PTR record:**
  ```
  utils network host ip-addr
  
  where ip-addr is the IP address of the server.
  
  For example:
  ```
  ```
  admin: utils network host 10.53.50.219
  Local Resolution:
  10.53.50.219 resolves locally to server1.new-domain.com
  
  External Resolution:
  server1.new-domain.com has address 10.53.50.219
  ```
Chapter 6      Modify Server Domain

Update IM and Presence Node Name

219.50.53.10.in-addr.arpa domain name pointer server1.new-domain.com.

| Note | At this point in the procedure, the Local Resolution result for the IP address will continue to point to the old FQDN value until the DNS domain is changed on the server. |

| c. | To validate any updated SRV records: |

```shell
tools network host srv-name srv
```
where `srv-name` is the SRV record.

The following example shows a `_xmpp-server` SRV record lookup:

```shell
tools network host _xmpp-server._tcp.galway-imp.com srv
```
Local Resolution:
Nothing found

| External Resolution: |

| _xmpp-server._tcp.sample.com has SRV record 0 0 5269 server1.new-domain.com. |

What To Do Next
Update IM and Presence Node Name, page 6-5

Update IM and Presence Node Name

If the node name defined for the server in Cluster Topology on the Cisco Unified CM IM and Presence Administration GUI is set to the Fully Qualified Domain Name (FQDN) of the server, then it references the old domain name. Therefore you must update the node name to reference the new domain name.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>• This procedure is only required if the node name value for this server is set to FQDN.</td>
</tr>
<tr>
<td>• If the node name matches the IP address or the hostname of the server then this procedure is not required.</td>
</tr>
</tbody>
</table>

If multiple servers within a cluster are being modified, you must complete the following procedure sequentially for each of these servers.

If the publisher node is being modified, you must complete this procedure for the subscriber node(s) first, before completing the procedure on the publisher node.

Before You Begin
Ensure that you updated the DNS records. See Update DNS Records, page 6-3 for more information.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Modify the node name for the IM and Presence server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Sign into the Cisco Unified CM IM and Presence Administration GUI on the server.</td>
</tr>
<tr>
<td>b.</td>
<td>Navigate to System &gt; Cluster Topology.</td>
</tr>
</tbody>
</table>
Update DNS Domain

This procedure outlines how to change the DNS domain of the server via the Administration CLI.

While this procedure modifies the DNS domain of the server, it does not attempt to modify the enterprise-wide presence domain, as configured on the Cluster Topology settings of the Cisco Unified CM IM and Presence Administration GUI.

Note

- The enterprise-wide presence domain does not need to align with the DNS domain of any IM and Presence server.
- If you wish to modify the enterprise-wide presence domain for your deployment, see Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager.

If multiple servers within a cluster are being modified, you must complete the following procedure sequentially for each of these servers.

If the publisher node is being modified, then you must complete this procedure on the publisher node first, before repeating on any applicable subscriber nodes.

Before You Begin

Ensure that you have updated the IM and Presence node name, see Update IM and Presence Node Name, page 6-5.
**Procedure**

**Step 1**  
Sign into the Administration CLI on the server and run the following command to change the domain:

```bash
set network domain new-domain
```

where `new-domain` is the new domain value to be set. Sample output is as follows:

```bash
admin: set network domain new-domain.com

*** WARNING ***
Adding/deleting or changing domain name on this server will break database replication. Once you have completed domain modification on all systems that you intend to modify, please reboot all the servers in the cluster. This will ensure that replication keeps working correctly. After the servers have rebooted, please confirm that there are no issues reported on the Cisco Unified Reporting report for Database Replication.

The server will now be rebooted. Do you wish to continue.

Security Warning: This operation will regenerate all CUP Certificates including any third party signed Certificates that have been uploaded.

Continue (y/n)?
```

**Step 2**  
Select y and the return key to confirm the domain change and reboot the server.

**Note**  
When the node name change is made, all certificates are regenerated on the server. If any of those certificates were signed by a third party Certificate Authority, then you must re-request those signed certificates later in the procedure, see Regenerate Security Certificates, page 6-11.

**Step 3**  
As mentioned in the above example, changing the domain name triggers an automatic reboot of the server. After the server has restarted run the following command to confirm the domain name change has taken effect:

```bash
show network eth0
```

For example, the following command confirms the new domain to be “new-domain.com”.

```bash
admin: show network eth0

Ethernet 0
DHCP : disabled     Status : up
IP Address : 10.53.50.219     IP Mask : 255.255.255.000
Link Detected: yes     Mode : Auto disabled, Full, 1000 Mbits/s
Duplicate IP : no

DNS
Primary : 10.53.51.234     Secondary : Not Configured
Options : timeout:5 attempts:2
Domain : new-domain.com
Gateway : 10.53.50.1 on Ethernet 0
```

**What To Do Next**  
Reboot all servers in the cluster, see Reboot all Servers in Cluster after Domain Update, page 6-8.
Reboot all Servers in Cluster after Domain Update

After the server(s) has been rebooted and has come back up, you must proceed to manually reboot all servers in the cluster (including those servers that just automatically rebooted). This reboot is to ensure that Operating System configuration files on all servers are aligned with the new domain values.

Initiate the reboot process on the publisher node first. When the publisher node has restarted, proceed to reboot the remaining subscriber nodes in any order.

Before You Begin
Ensure that you have changed the DNS domain of the server, see Update DNS Domain, page 6-6.

Procedure

Step 1
Reboot the publisher from the Administration CLI with the following command:

```bash
utils system restart
```

The following output displays:

```
admin: utils system restart
Do you really want to restart ?
Enter {yes/no)?
```

Step 2
Enter yes and select return to restart.

Step 3
Wait until you see the following message that indicates the publisher node has restarted:

```
The system is going down for reboot NOW!
Waiting .
Operation succeeded
restart now.
```

Step 4
Reboot each subscriber node by signing into the Administration CLI on that node and running the same command:

```bash
utils system restart
```

Note
After a number of minutes trying to stop services, the admin CLI may ask you to force a restart. If this occurs, enter yes.

What To Do Next
Restart database replications, see Restart Database Replication, page 6-9.
Restart Database Replication

After all the servers within the cluster have been restarted, you must restart database replication.

Note

Restarting database replication may take up to and over an hour to complete if the cluster has a large number of licensed users. Use the validation mechanisms listed in the following procedure to ensure replication is complete on all nodes before moving to the next step.

Before You Begin

Ensure that you rebooted all servers in the cluster, see Reboot all Servers in Cluster after Domain Update, page 6-8.

Procedure

Step 1

On all nodes in the cluster, validate that the required database services are running by entering the following command from the Administration CLI:

```
utils service list
```

The following output displays

```
admin: utils service list

Requesting service status, please wait...
System SSH [STARTED]
Cluster Manager [STARTED]
Service Manager is running
Getting list of all services
>> Return code = 0
A Cisco DB[STARTED]
A Cisco DB Replicator[STARTED]
Cisco AMC Service[STARTED]
Cisco AXL Web Service[STARTED]
Cisco Audit Event Service[STARTED]
Cisco Bulk Provisioning Service[STARTED]
Cisco CDP[STARTED]
--
--
Cisco XCP Authentication Service[STARTED]
Cisco XCP Config Manager[STARTED]
Cisco XCP Connection Manager[STARTED]
Cisco XCP Directory Service[STARTED]
Cisco XCP Router[STARTED]
Cisco XCP SIP Federation Connection Manager[STARTED]
Cisco XCP Text Conference Manager[STARTED]
Cisco XCP Web Connection Manager[STARTED]
Cisco XCP XMPP Federation Connection Manager[STARTED]
Host Resources Agent[STARTED]
MIB2 Agent[STARTED]
Platform SOAP Services[STARTED]
SNMP Master Agent[STARTED]
SOAP -Log Collection APIs[STARTED]
SOAP -Performance Monitoring APIs[STARTED]
SOAP -Real-Time Service APIs[STARTED]
System Application Agent[STARTED]
Cisco XCP Message Archiver[STOPPED] Service Not Activated
```
Primary Node = true

**Step 2**  
From the output, ensure that the following services are in a STARTED state:
- A Cisco DB
- A Cisco DB Replicator
- Cisco Database Layer Monitor

**Note**  
Do not proceed beyond this point until the above services are running on all nodes in the cluster.

**Step 3**  
On the publisher node, run the following command from the Administration CLI to restart replication across the cluster:
```
utils dbreplication reset all
```

The following output displays:
```
admn: utils dbreplication reset all  
This command will try to start Replication reset and will return in 1-2 minutes. 
Background repair of replication will continue after that for 1 hour. 
Please watch RTMT replication state. It should go from 0 to 2. When all subs have an RTMT Replicate State of 2, replication is complete. 
If Sub replication state becomes 4 or 1, there is an error in replication setup. 
Monitor the RTMT counters on all subs to determine when replication is complete. 
Error details if found will be listed below
```
OK [10.53.50.219]

It may take 1-2 minutes for this CLI command to return. However, replication recovery will continue to run in the background and may take much longer than 1-2 minutes.

**Step 4**  
Verify that replication was successfully established on the publisher node by running the following command from the Administration CLI:
```
utils dbreplication runtimestate
```

The following output displays:
```
admn: utils dbreplication runtimestate  
DDB and Replication Services: ALL RUNNING

DB CLI Status: No other dbreplication CLI is running...

Cluster Replication State: BROADCAST SYNC Completed on 1 servers at: 2012-09-26-15-18
  Last Sync Result: SYNC COMPLETED 257 tables sync'ed out of 257
  Sync Errors: NO ERRORS

DB Version: ccm9_0_1_10000_9000
Number of replicated tables: 257
Repltimeout set to: 300s

Cluster Detailed View from gwydlvm020105 (2 Servers):

<table>
<thead>
<tr>
<th>SERVER-NAME</th>
<th>IP ADDRESS</th>
<th>PING (msec)</th>
<th>RPC?</th>
<th>REPLICA TION STATUS</th>
<th>REPL. QUEUE</th>
<th>DBVER&amp; TABLES</th>
<th>REPL. LOOP?</th>
<th>REPLICA TION SETUP (RTMT) &amp; details</th>
</tr>
</thead>
<tbody>
<tr>
<td>server1</td>
<td>192.168.10.201</td>
<td>0.038</td>
<td>Yes</td>
<td>Connected</td>
<td>0</td>
<td>match</td>
<td>Yes</td>
<td>(2) PUB Setup Completed</td>
</tr>
<tr>
<td>server2</td>
<td>192.168.10.202</td>
<td>0.248</td>
<td>Yes</td>
<td>Connected</td>
<td>0</td>
<td>match</td>
<td>Yes</td>
<td>(2) Setup Completed</td>
</tr>
<tr>
<td>server3</td>
<td>192.168.10.203</td>
<td>0.248</td>
<td>Yes</td>
<td>Connected</td>
<td>0</td>
<td>match</td>
<td>Yes</td>
<td>(2) Setup Completed</td>
</tr>
<tr>
<td>server3</td>
<td>192.168.10.204</td>
<td>0.248</td>
<td>Yes</td>
<td>Connected</td>
<td>0</td>
<td>match</td>
<td>Yes</td>
<td>(2) Setup Completed</td>
</tr>
</tbody>
</table>
Step 5

Repeat Step 3 until all nodes show a replication status of **Connected** and a replication setup value of **(2)**. **Setup Complete.** At this point, the publisher node considers database replication as fully established.

*Note*

If a Replication Setup value of **(4)** is shown for any server there may be a replication issue. Return to Step 1 of this procedure to restart replication again.

---

Step 6

Verify that replication was successfully established on all subscriber nodes by running the following command from the Administration CLI of each node:

```plaintext
utils dbreplication runtimestate
```

---

Step 7

Repeat Step 6 until all nodes show a replication status of **Connected** and a replication setup value of **(2)**. At this point, the subscriber node considers database replication as fully established.

*Note*

If a Replication Setup value of **(4)** is shown for any server there may be a replication issue. Return to Step 1 of this procedure to restart replication again.

When replication has been successfully established on all nodes, this procedure to restart database replication is complete.

---

**What To Do Next**

Regenerate Security Certificates, page 6-11.

---

**Regenerate Security Certificates**

The Fully Qualified Domain Name (FQDN) of the server is used as Subject Common Name in all IM and Presence security certificates. Therefore, when the DNS domain is updated on a server, all security certificates are automatically regenerated.

If any certificates were signed by a third party Certificate Authority, then you must manually generate new Certificate Authority signed certificates.

If multiple servers within a cluster are being modified, you must complete the following procedure for each of these servers.

**Before You Begin**

Ensure that database replication has been successfully established on all nodes, see Restart Database Replication, page 6-9.

**Procedure**

**Step 1**

If a certificate must be signed by a third party Certificate Authority, sign into the Cisco Unified IM and Presence Operating System Administration GUI and perform the required steps for each relevant certificate.

**Step 2**

After you upload the signed certificate, you may need to restart services on the IM and Presence server. The required service restarts are as follows:

- **Tomcat certificate**—restart the tomcat service by running the following command from the Administration CLI:
utils service restart tomcat

- **Cup-xmpp certificate**—restart the Cisco XCP Router service from the Cisco Unified IM and Presence Serviceability GUI.

- **Cup-xmpp-s2s certificate**—restart the Cisco XCP Router service from the Cisco Unified IM and Presence Serviceability GUI.

---

**Note**

- These restarts are service-impacting. Therefore, depending on the time lag in acquiring the signed certificates, you may need to schedule a later maintenance window to restart these services. In the meantime, the self-signed certificates will continue to be presented on the relevant interfaces until the services are restarted.

- If a certificate is not specified in the list above, then no service restarts are required for that certificate.

---

**What To Do Next**

Complete the post-change task list on all applicable nodes within the cluster, see Post-Change Task List, page 7-1.
CHAPTER 7

Post-Change Task List

May 14, 2014

Complete this procedure after you finish changing the IP address, hostname or domain of your cluster.

Procedure

**Step 1** Ensure that all servers in the cluster are running and available by checking for any active ServerDown alerts. You can check the application event log for ServerDown alerts by entering the following command in the Command Line Interface (CLI) on the publisher node:

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

**Step 2** Check the DB replication status on all the IM and Presence nodes in the cluster to ensure all servers are replicating database changes successfully. You can check by using the following CLI command.

```
utils dbreplication runtimestate
```

**Note** The REPLICATION SETUP (RTMT) & details value for all nodes must be 2.

**Step 3** If you completed Step 9 in the Readiness Checklist, add the cluster whose publisher/subscriber hostname/IP address was changed to each peer-cluster publisher node.

**Step 4** If you disabled SSO prior to performing a procedure, you can enable it now. For information about how to enable SSO, see the “Single Sign-On Configuration” section of *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

**Step 5** Run a manual DRS backup and ensure that all nodes and active services are backed up successfully.

**Step 6** If the IP address for the server has been changed, 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 7** 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.
- SIP trunks
- SFTP servers that are used for IM and Presence server trace collection or as a DRS backup destination
- Cisco Jabber
- Associated routers and gateways
- Third-party clients, such as IBM Lotus Sametime

**Step 8**  
On all nodes, verify that services are running. If you need to start services, use the following commands to start the IM and Presence services in the following order:

- `utils service start Cisco XCP Config Manager`
- `utils service start Cisco Route Datastore`
- `utils service start Cisco Login Datastore`
- `utils service start Cisco SIP Registration Datastore`
- `utils service start Cisco Presence Datastore`
- `utils service start Cisco XCP Router`
- `utils service start Cisco Sync Agent`
- `utils service start Cisco SIP Proxy`
- `utils service start Cisco OAM Agent`
- `utils service start Cisco Presence Engine`
- `utils service start Cisco Client Profile Agent`
- `utils service start Cisco Intercluster Sync Agent`
- `utils service start Cisco Config Agent`

**Step 9**  
If High Availability (HA) was disabled before the hostname or IP address change, enable HA on all subclusters. Select **System > Cluster Topology** in Cisco Unified CM IM and Presence Administration. For more information about how to enable HA, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

**Step 10**  
You must run a manual DRS backup after you change the IP address or hostname 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.

---

**Related Topics**

- *Disaster Recovery System Guide*
- *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*
Perform the steps in this procedure only if you change the hostname or IP address on a IM and Presence server that was previously integrated with Microsoft LCS/OCS. You need to do this to ensure the Microsoft Office Communicator (MOC) server and clients reflect the correct IM and Presence IP address and hostname (after your changes) and the new FQDN.

Before You Begin
Complete the Post-Change Task List.

Procedure

Step 1 Sign out of any existing MOC client session that you may have running.

Step 2 Sign in to the OCS or LCS server.

Step 3 Edit the Front End properties, in the following tabs on the OCS or LCS server:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Action</th>
</tr>
</thead>
</table>
| Routing Tab             | a. Update the renamed IM and Presence server with its new FQDN and IP address.  
                          | b. Change the ‘Next Hop’ IP address of the wildcarded IM and Presence domain to be the new IM and Presence IP address. |
| Host Authorization Tab  | Ensure that the new IM and Presence IP address and new FQDN is listed as follows: |
|                         | • Outbound only – N                                                   |
|                         | • Throttle As Server – Y                                             |
|                         | • Treat As Authenticated - Y                                         |

Step 4 Right-click on the LCS/OCS Users, and edit as follows:

a. Change the ‘Server URI’ to be the new IM and Presence FQDN.

b. Select OK.

Step 5 Stop the OCS/LCS Front End Service.
Step 6  Restart the OCS/LCS Front End Service.
Step 7  Sign in to the MOC client, and confirm control of a Cisco device.

Related Topics
- Integration Note for Configuring IM and Presence with Microsoft OCS for MOC Call Control
- Post-Change Task List, page 7-1
Obtaining Documentation, Obtaining Support, and Security Guidelines

May 14, 2014

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:


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