Domain Name and Node Name Changes

- Domain Name Change, on page 1
- Node Name Change, on page 9
- Update Domain Name for Cisco Unified Communications Manager , on page 12

Domain Name Change

Administrators can modify the network-level DNS default domain that is associated with an IM and Presence Service node or group of nodes.

The enterprise-wide IM and Presence Service domain does not need to align with the DNS default domain of any IM and Presence Service node. To modify the enterprise-wide domain for your deployment, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager Configuration and Administration Guide for the IM and Presence Service*.

Caution Changing the default domain on any node in an IM and Presence Service cluster will result in node 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.

When you change the default domain name for a node, all third-party signed security certificates are automatically overwritten with new self-signed certificates. If you want to have those certificates re-signed by your third-party Certificate Authority, you must manually request and upload the new certificates. Service restarts may be required to pick up these new certificates. Depending on the time that is required to request new certificates, a separate maintenance window may be required to schedule the service restarts.

Note New certificates cannot be requested in advance of changing the default domain name for the node. Certificate Signing Requests (CSRs) can only be generated after the domain has been changed on the node and the node has been rebooted.

IM and Presence Service Default Domain Name Change Tasks

The following table contains the step-by-step instructions for modifying the network-level DNS default domain name associated with an IM and Presence Service node or group of nodes. 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.

Procedure

Step 1 Complete the pre-change tasks on all applicable nodes within the cluster. Some of the pre-change tasks may apply only to the IM and Presence database publisher node and can be skipped if you are modifying a subscriber node.

Step 2 Update the DNS records for the IM and Presence Service node on all applicable nodes within the cluster. Also update SRV, Forward (A), and Reverse (PTR) records as appropriate to incorporate the new node domain.

Step 3 Update the IM and Presence Service node name on all applicable nodes within the cluster using Cisco Unified Communications Manager Administration.

Note
This step is mandatory for the FQDN node name format. It is not applicable if the node name is an IP address or a Hostname.

- If the node name is an FQDN, then it references the old node domain name. Therefore, you must update the node name such that the FQDN value reflects the new domain name.
- If the node name is an IP address or hostname, then the domain is not referenced and therefore no changes are required.

Step 4 Update the DNS domain on all applicable nodes using the Command Line Interface (CLI). The CLI command makes the required domain change on the node operating system and triggers an automatic reboot of each node.

Step 5 Restart the 'A Cisco DB' service of all the nodes in the cluster after the domain name update to ensure that operating system configuration files on all nodes pick up the DNS domain name change that is associated with the modified nodes.

Note
Verify that the system is working properly. If you observe any replication issues, ensure that you restart all the nodes in the cluster.

Step 6 Verify database replication using the CLI. See topics related to performing system health checks and troubleshooting database replication for details. After all system files are synchronized within the cluster, you must verify database replication.

Step 7 Regenerate security certificates on the node.

- The Subject Common Name on all IM and Presence Service security certificates is set to the node FQDN. Therefore, to incorporate the new node domain, all certificates are automatically regenerated after a DNS domain change.
- Any certificates that were previously signed by a certificate.

Step 8 Complete the post-change tasks for all applicable nodes within the cluster to ensure that the cluster is fully operational.

Update DNS Records

Because you are changing the DNS domain for the node, you must also update any existing DNS records associated with that node. This includes the following types of records:

- A records
- PTR records
- SRV records

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

If you are modifying the IM and Presence database publisher node, you must complete this procedure on the IM and Presence database publisher node first before repeating on any applicable IM and Presence Service subscriber nodes.

Note

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

Before you begin

Perform all pre-change tasks and the applicable system health checks on your deployment.

Procedure

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

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

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

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

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

Step 6 Verify that all the above DNS changes have propagated to all other nodes within the cluster by running the following Command Line Interface (CLI) command on each node:

a) To validate the new A record, enter **utils network host new-fqdn**, where `new-fqdn` is the updated FQDN of the node.

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
```

b) To validate the updated PTR record, enter **utils network host ip-addr**, where `ip-addr` is the IP address of the node.

```
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
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 node.

c) To validate any updated SRV records, enter **utils network host srv-name srv**, where `srv-name` is the SRV record.

Example:

_xmpp-server SRV record lookup example.

```
admin: utils 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 the IM and Presence Service node name.

Update Node Name in FQDN Value

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

Note This procedure is only required if the node name value for this node is set to FQDN. If the node name matches the IP address or the hostname of the node, then this procedure is not required.

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

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

Before you begin

Update the DNS records for the node.

Procedure

Step 1 Modify the node name for the IM and Presence Service node.

a) Sign in to Cisco Unified Communications Manager Administration.
b) Select **System** > **Server**.
c) Search for and select the node.
d) Update the **Fully Qualified Domain Name/IP Address** field so that the FQDN references the new domain value. For example, update the **Fully Qualified Domain Name/IP Address** value from `server1.old-domain.com` to `server1.new-domain.com`.
e) Select **Save**.

Step 2 Verify that the Application Server entry for this node has been updated to reflect the new node name on the **Presence Topology** window of the Cisco Unified CM IM and Presence Administration GUI.

a) Sign in to Cisco Unified Communications Manager Administration and select **System** > **Application Server**.
b) Click **Find**, if required, on the **Find and List Application Servers** window.
c) Ensure that an entry exists for the updated node name in the list of Application Servers.

Note
Do not continue if there is no entry for this node or if there is an entry but it reflects the old node name for the node.

What to do next

Update the DNS domain on all applicable nodes.

Update DNS Domain

You can change the DNS domain of the IM and Presence Service node using the Command Line Interface (CLI).

The enterprise-wide IM and Presence Service domain does not need to align with the network-level DNS default domain of any IM and Presence Service node. To modify the enterprise-wide domain for your deployment, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

If you are modifying multiple nodes within a cluster, then you must complete the following procedure sequentially for each node.

If you are modifying the IM and Presence database publisher node, then you must first complete this procedure on the database publisher node before you modify any subscriber nodes.

Before you begin

Update the IM and Presence Service node name.

Procedure

Step 1 Sign in to the CLI on the node and enter **`set network domain new-domain`**, where `new-domain` is the new domain value to be set.

Example:

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

*** W A R N I N G ***
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 service is 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 Enter **`y`** and press **Return** to confirm the domain change and restart of the node or enter **`n`** to cancel.

Tip
When the node name change is complete, all certificates are regenerated on the node. 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.

Step 3 After the node restarts, enter `show network eth0` to confirm the domain name change has taken effect.

Example:

The new domain in the following example is new-domain.com.

```
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
```

Step 4 Repeat the previous steps on all applicable nodes in the cluster.

What to do next

Reboot all nodes in the cluster.

Cluster Nodes Considerations

You can use the Command Line Interface (CLI) to restart the "A Cisco DB" service in the nodes in your cluster.

After you change the domain name and the node reboots, you need to restart the 'A Cisco DB' service of all the nodes in the cluster, including those nodes that have automatically rebooted, starting with the Unified CM publisher and then for all the subscribers as the published database comes up. This ensures that the Operating System configuration files on all nodes are aligned with the new domain values.

Verify that the system is working properly. If you observe any replication issues, ensure that you restart all the nodes in the cluster.

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

Before you begin

Ensure that the DNS domain name of the node was changed.

Procedure

Step 1 Reboot the IM and Presence database publisher node using the CLI. Enter **`utils system restart`**.

Example:

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

Step 2 Enter **`yes`** and press **Return** to restart.

Step 3 Wait until you see the following message that indicates the IM and Presence database publisher node has restarted.

Example:

```
Broadcast message from root (Wed Oct 24 16:14:55 2012):

The system is going down for reboot NOW!
Waiting .

Operation succeeded

restart now.
```

Step 4 Sign in to the CLI on each IM and Presence Service subscriber node and enter **utils system restart** to reboot each subscriber node.

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

What to do next

Verify database replication. See topics related to system health checks for more information.

Regenerate Security Certificates

The Fully Qualified Domain Name (FQDN) of the node is used as Subject Common Name in all IM and Presence Service security certificates. Therefore, when the DNS domain is updated on a node, 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 you are modifying multiple nodes within a cluster, you must complete the following procedure for each node.

Note New certificates cannot be requested in advance of changing the default domain name for the node. Certificate Signing Requests (CSRs) can only be generated after the domain has been changed on the node and the node has been rebooted.

Before you begin

Verify database replication to ensure that database replication is successfully established on all nodes.

Procedure

Step 1 If a certificate must be signed by a third-party Certificate Authority, sign in to the Cisco Unified 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 Service node.

The required service restarts are as follows:

- Tomcat certificate: Restart the tomcat service by running the following Command Line Interface (CLI) command:

```
utils service restart Cisco Tomcat
```

- Cup-xmpp certificate: Restart the Cisco XCP Router service from the Cisco Unified Serviceability GUI.
- Cup-xmpp-s2s certificate: Restart the Cisco XCP Router service from the Cisco Unified Serviceability GUI.

Note

- These actions restart the affect service. Therefore, depending on the time lag in acquiring the signed certificates, you may need to schedule the restarts for a later maintenance window. 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 preceding list, no service restarts are required for that certificate.

What to do next

Perform the post-change task list on all applicable nodes within the cluster.

Node Name Change

You can modify the node name that is associated with an IM and Presence Service node or group of nodes. The updates are displayed on the **Server Configuration** window of Cisco Unified Communications Manager Administration.

Use these procedures for 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

For more information about node name recommendations, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Caution Use this procedure to change the node name only for an IM and Presence Service node where there are no network-level changes needed. Perform the procedures that are specific to changing the network IP address, hostname, or the domain name in that case. You must perform this node name change procedure during a scheduled maintenance window. Changing the node name on any node in an IM and Presence Service cluster will result in node restarts and interruptions to presence services and other system functions.

IM and Presence Service Node Name Change Task List

The following table contains the step-by-step instructions to change the node name that is associated with an IM and Presence Service 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, complete all the sequential steps to change the node name on one cluster at a time.

Table 1: Change IM and Presence Service Node Name Task List

Item	Task
1	Complete the pre-change tasks on all applicable nodes within the cluster. Some of the pre-change tasks may apply only to the IM and Presence database publisher node and can be skipped if you are modifying a subscriber node.
2	Update the IM and Presence Service node name using Cisco Unified Communications Manager Administration.
3	Verify the node name updates and ensure that the node name change is synchronized with IM and Presence Service.
4	Verify database replication using the Command Line Interface (CLI) after the node name updates are complete. Ensure that the new node names have replicated across the cluster and that database replication is operational on all nodes.
5	Complete the post-change tasks list on the updated nodes and verify that the node is fully functional.

Update Node Name

If multiple nodes within a cluster are being modified, you must complete the following procedure sequentially for each node.

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

Note For IM and Presence nodes, it's recommended to use a fully qualified domain name. However, IP addresses and hostnames are also supported.

Before you begin

Perform all pre-change tasks and the applicable system health checks for your deployment.

Procedure

Step 1 Sign in to Cisco Unified CMAdministration.

Step 2 Select **System** > **Server**.

Step 3 Select the node that you want to modify.

Step 4 Update the **Host Name/IP Address** field with the new node name.

Note
Ensure you upload the newly generated SP metadata to the IDP server.

Step 5 If multiple nodes within a cluster are being modified, repeat this procedure for each node.

Note
If you update the IM and Presence Service node name and you also have third-party compliance configured, you must update the compliance server to use the new realm which is based on the node name. This configuration update is made on the third-party compliance server. The new realm will be displayed on the **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Compliance** > **Compliance Settings** window.

What to do next

Verify the node name change.

Verify Node Name Changes Using CLI

You can verify that the new node name has replicated across the cluster using the Command Line Interface (CLI).

Procedure

Step 1 Enter **`run sql name select from processnode`** to validate that the new node name has replicated correctly on each node in the cluster.

Example:

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

Step 2 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.

a) If the output is as expected, then validation has passed and you do not need to validate database replication for the nodes.

b) If any new node names are missing or if there are peferences to old node names, then continue to Step 3.

Step 3 To troubleshoot missing node names or old node names that appear for the node, perform the following actions:

a) For an IM and Presence database publisher node, check if the sync agent is running ok and verify that there are no errors in the sync agent status using the dashboard on the Cisco Unified CM IM and Presence Administration GUI.
b) For subscriber nodes, perform the validate database replication procedure.

Verify Node Name Changes Using Cisco Unified CM IM and Presence Administration

For IM and Presence Service nodes only, verify that the application server entry for this node has been updated to reflect the new node name on Cisco Unified CM IM and Presence Administration GUI.

Before you begin

Update the IM and Presence Service node name.

Procedure

Step 1 Sign in to the Cisco Unified CM IM and Presence Administration GUI.
Step 2 Select **System** > **Presence Topology**.
Step 3 Verify that the new node name appears in the **Presence Topology** pane.

What to do next

Verify database replication.

Update Domain Name for Cisco Unified Communications Manager

You can use the Command Line Interface (CLI) to change the domain name for Cisco Unified Communications Manager. Update the DNS domain name on all applicable nodes using the CLI. The CLI command makes the required domain name change on the node and triggers an automatic reboot for each node.

If the Unified CM cluster security mode is non-secure and you are updating or changing the domain, then as a part of domain changes all certificates will be regenerated. To make sure that the ITLs are updated on the phones, perform the following steps needed prior to updating the domain name:

1. Ensure that all phones are online and registered so that they can process the updated ITLs. For phones that are not online when this procedure is performed, the ITL must be deleted manually.
2. Set the **Prepare Cluster for Rollback to pre-8.0 enterprise** parameter to **True**. All phones automatically reset and download an ITL file that contains empty Trust Verification Services (TVS) and TFTP certificate sections.

3. On the phone, select **Settings** > **Security** > **Trust List** > **ITL File** to verify that the TVS and TFTP certificate sections of the ITL file are empty.
4. Change the domain of the server and let the phones configured for rollback register to the cluster.
5. After all the phones have successfully registered to the cluster, set the enterprise parameter **Prepare Cluster for Rollback to pre-8.0** to **False**.

Before you begin

- Ensure to enable the DNS before changing the domain name.
- Sign in to Cisco Unified Communications Manager Administration and navigate to the **System** > **Server Fields** page. If this server configuration settings page has an existing hostname entry, you should first change the hostname entry of the domain name.
- Perform all pre-change tasks and the applicable system health checks. See the Related Topic section for more information.

Procedure

Step 1 Log in to Command Line Interface.

Step 2 Enter **run set network domain <new_domain_name>**.
The command prompts for a system reboot.

Step 3 Click **Yes** to reboot the system.
The new domain name gets updated after the system is rebooted.

Step 4 Enter the command **show network eth0** to check if the new domain name is updated after the reboot.

Step 5 Repeat this procedure for all cluster nodes.

What to do next

Perform all applicable post-change tasks to ensure that your changes are properly implemented in your deployment.