Change Server Domain

Procedure Overview

This procedure allows an administrator to modify the DNS domain that is associated with a Cisco Unified Presence server or group of servers.

Caution Changing the domain on any server in a Cisco Unified 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 modify the enterprise-wide presence domain, as configured on the Cluster Topology settings of the Cisco Unified Presence Administration GUI.

- The enterprise-wide presence domain does not need to align with the DNS domain of any Cisco Unified Presence server.
- If you want to modify the enterprise-wide presence domain for your deployment, see the *Deployment Guide for Cisco Unified Presence*.

Note

- This procedure results in all third-party signed security certificates being 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.
- 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 a Cisco Unified 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 6-1 Workflow to modify the DNS domain

Step	Task	Node Name Format		
		IP Address	Hostname	FQDN
1	**Complete the Pre-Change Tasks on all applicable nodes within the cluster.** • This procedure includes several prerequisite steps, including a list of services that you must 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.	X	X	X
2	**Update DNS Records for the server on all applicable nodes within the cluster.** • Update SRV, Forward (A), and Reverse (PTR) records as appropriate to incorporate the new server domain.	X	X	X

Table 6-1 Workflow to modify the DNS domain

Step	Task	Node Name Format		
		IP Address	Hostname	FQDN
3	**Update Cisco Unified Presence Node Name on all applicable nodes within the cluster from the Cisco Unified Presence Administration GUI.** • If the node name is an FQDN, then it references the old server domain name. Therefore, you must update the node name such that the FQDN value reflects the new server domain. • If the node name is an IP address or hostname, then the domain is not referenced and therefore no changes are required.	NA	NA	X
4	**Update DNS Domain on all applicable nodes from the Administration CLI.** This CLI command makes the required domain change on the server operating system. It will trigger an automatic reboot of each server.	X	X	X
5	**Reboot all Servers in Cluster after Domain Update.** This step ensures that operating system configuration files on all nodes pick up the DNS domain change that is associated with the modified servers.	X	X	X
6	**Verify Database Replication from the Administration CLI.** After all system files are in sync within the cluster, you must verify database replication.	X	X	X
7	**Regenerate Security Certificates on the server.** • The Subject Common Name on all Cisco Unified Presence security certificates is set to the server FQDN. Therefore, to incorporate the new server domain, all certificates are automatically regenerated after a DNS domain change. • Any certificates that were previously signed by a Certificate Authority will need to be manually re-signed.	X	X	X
8	**Complete the Post-Change Tasks list on all applicable nodes within the cluster.** Perform a series of steps to ensure the cluster is operational again.	X	X	X

Update DNS Records

Because you are changing the DNS domain for the server, you must also update any existing DNS records associated with that server. 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 you are modifying the publisher node, 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 Cisco Unified Presence Service functionality.

Before You Begin

Ensure that you have completed the pre-change tasks. See Pre-Change Tasks, page 3-1 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 sever 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:

a. 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
```

b. 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
```

```
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:

utils network host *srv-name* srv

where *srv-name* is the SRV record.

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

```
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 Cisco Unified Presence Node Name, page 6-5

Update Cisco Unified Presence Node Name

If the node name defined for the server in Cluster Topology on the Cisco Unified 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.

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

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

Step 1 Modify the node name for the Cisco Unified Presence server.

a. Sign into the Cisco Unified Presence Administration GUI on the server.

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

c. 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, with the **Fully Qualified Domain Name/IP Address** field set to the FQDN of the server.

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 server has been updated to reflect the new node name on the Cisco Unified Communications Manager Administration GUI.

a. Sign into the Cisco Unified Communications Manager Administration GUI and Navigate to **System > Application Server**.

b. Click **Find**, if required, on the **Find and List Application Servers** page.

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 server or if there is an entry but it reflects the old node name for the server.

What To Do Next

Update the DNS Domain on all applicable nodes. See Update DNS Domain, page 6-6.

Update DNS Domain

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

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

Note

- The enterprise-wide presence domain does not need to align with the DNS domain of any Cisco Unified Presence server.
- If you want to modify the enterprise-wide presence domain for your deployment, see the *Deployment Guide for Cisco Unified Presence*.

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 Cisco Unified Presence node name. See Update Cisco Unified Presence Node Name, page 6-5.

Procedure

Step 1 Sign in to the Administration CLI on the server and run the following command to change the domain

set network domain *new-domain*

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

```
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 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 select the **Return** key to confirm the domain change and reboot the server.

Note When the node name change is complete, 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 After the server restarts run the following command to confirm the domain name change has taken effect:

show network eth0

For example, the following command confirms the new domain to be “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 Steps 1 to 3 on all applicable nodes in the cluster.

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 has been rebooted, you must 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:

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:

```
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 Reboot each subscriber node by signing in to the Administration CLI on that node and running the same command:

utils system restart

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

What To Do Next

Verify Database Replication, page 6-9.

Verify Database Replication

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

Note Use the validation mechanisms that are listed in the following procedure to ensure that replication is complete on all nodes before you proceed 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
```

Tip The output of the `utils service list` command is very long. To view the output page by page, enter the command `utils service list page`.

```
The following output displays:
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

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

Step 3 Verify that replication has been successfully established on the publisher node by running the following command from the Administration CLI:

utils dbreplication runtimestate

The following 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):
                      PING       REPLICATION    REPL.   DBver&   REPL.  REPLICATION SETUP
SERVER-NAME  IP ADDRESS      (msec)  RPC?   STATUS          QUEUE   TABLES   LOOP?  (RTMT) & details
-----------  --------------   ------  ----   ------------   -----    ------  -----   -----------------
server1     192.168.10.201   0.038   Yes    Connected     0        match   Yes     (2) PUB Setup Completed
server2      192.168.10.202   0.248   Yes    Connected     0        match   Yes     (2) Setup Completed
server3      192.168.10.203   0.248   Yes    Connected     0        match   Yes     (2) Setup Completed
server4      192.168.10.204   0.248   Yes    Connected     0        match   Yes     (2) Setup Completed
```

Step 4 Repeat Step 3 until all nodes show a replication status of **Connected** and a replication setup value of **(2) Setup Complete**. At this point, database replication on the publisher node is fully established.

Step 5 Verify that replication has been successfully established on all subscriber nodes by running the following command from the Administration CLI of each node:

utils dbreplication runtimestate

Step 6 Repeat Step 5 until all nodes show a replication status of **Connected** and a replication setup value of **(2) Setup Complete**. At this point, database replication on the subscriber node is fully established.

When database replication has been successfully verified on all nodes, this step in the procedure is complete.

Regenerate Security Certificates

The Fully Qualified Domain Name (FQDN) of the server is used as Subject Common Name in all Cisco Unified 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 you are modifying multiple servers within a cluster, 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 Verify Database Replication, page 6-9.

Procedure

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

- **Cup-xmpp certificate**—Restart the Cisco UP XCP Router service from the Cisco Unified Presence Serviceability GUI.
- **Cup-xmpp-s2s certificate**—Restart the Cisco UP XCP Router service from the Cisco Unified Presence Serviceability GUI.

Note

- These restarts affect service. 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 preceding list, 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 Tasks, page 8-1.