Change CUCM Server Definition from IP Address or Hostname to FQDN Format

Contents

Introduction

This document describes a procedure how to change definition of Cisco Unified Communications Manager (CUCM) cluster from IP address or hostname format to a Fully Qualified Domain Name (FQDN) format.

Background

CUCM has an option to choose whether to use IP addresses or Domain Name Service (DNS) in order to communicate between nodes and with endpoints.

For pre-10.x systems the recommendation was not to use DNS reliance unless it is required by specific design or requirements.

Starting from CUCM 10.x due to tight integration between CUCM and Cisco Unified Communications Manager IM & Presence Service (IM&P) that recommendation has changed. While not using DNS in basic IP telephony deployments is still acceptable, usage of fully qualified domain names instead of IP addresses became a requirement for some key features to work:

- Single Sign-On (SSO)
- Jabber deployments requiring user registration auto-discovery
- Certificate-based security for secure signaling and media

In order to set up a secure connection, a client needs to verify the identity of the server that presents the certificate.

The client performs the validation in two steps:

- At the first step the client checks if the server certificate is trusted by looking into its trust store. If this identity certificate or a Certificate Authority certificate, which was used to sign the

identity certificate, is present in the client's trust store, the certificate is considered as trusted.
- At the second step the client checks the idenitity of the server in the certificate against the identity of the server in local client configuration. In other words, the client verifies that server name in the certificate and the connection request is the same.

Identity of the server in the certificate is derived from Common Name attribute (CN) or Subject Alternative Name (SAN) attribute of the received certificate.

Note: SAN, if present, takes precedence over CN.

The identity of the server in local configuration is derived from the device configuration file downloaded via Trivial File Transfer Protocol (TFTP) and/or from User Data Services (UDS) interactions. TFTP and UDS services derive this configuration from the database **processnode** table. It can be configured in **CM Administration** > **System** > **Server** web page.

Do not confuse CM Administration > System > Server page, where servers are being defined, with OS Administration > Settings > IP Ethernet, where network parameters for servers are being configured. Parameters at OS Administration page affect actual network configuration of the server; hostname or domain change leads to regeneration of all certificates for the node. Settings at CM Administration page define, how CUCM advertises itself to endpoints via configuration files or UDS. Change of this setting does not require certificates regeneration. This setting must match one of the following network parameters of the node: IP address, hostname or FQDN.

For example, your endpoint securely connects to server.mydomain.com. It looks at the received certificate and verifies if "server.mydomail.com" is present in this certificate as CN or SAN. If the check does not succeed, the connection either fails or an end user gets a popup message, asking to accept untrusted certificate, depending on client functionality. Since CNs and SANs in certificates typically have FQDN format, you need to change the server definition from IP address to FQDN format, if you want to avoid these popups or connection failures.

Prerequisites

Requirements

Components Used

The information in this document is based on these software and hardware versions:

- CUCM 10.X or higher

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Procedure

Pre-Change Tasks

Before the configuration it is highly recommended to ensure that the prerequisites are met.

Step 1. Check DNS configuration.

Run these commands from CUCM CLI to ensure that DNS service is configured and FQDN entries for node names can be resolved both locally and externally.

```
admin:show network eth0
<omitted for brevity>

DNS
Primary : 10.48.53.194 Secondary : Not Configured
Options : timeout:5 attempts:2
Domain : mydomain.com
Gateway : 10.48.52.1 on Ethernet 0



admin:utils network host cucm105pub.mydomain.com
Local Resolution:
cucm105pub.mydomain.com resolves locally to 10.48.53.190

External Resolution:
cucm105pub.mydomain.com has address 10.48.53.190
admin:
```

Step 2. Network diagnostic test.

Ensure that network diagnostic test is passed by running this CLI command.

```
admin:utils diagnose module validate_network

Log file: platform/log/diag3.log

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

Diagnostics Completed
```

Step 3. DHCP configuration for endpoints.

Ensure that necessary Dynamic Host Configuration Protocol (DHCP) configuration is added for the registered phones to be able to do DNS resolution.

Step 4. Database replication.

Ensure that CUCM database replication is working. Cluster replication state must be **2** for all nodes.

```
admin:utils dbreplication runtimestate
<output omitted for brevity>
Cluster Detailed View from cucm105pub (2 Servers):
 PING DB/RPC/ REPL. Replication REPLICATION SETUP
SERVER-NAME IP ADDRESS (msec) DbMon? QUEUE Group ID (RTMT) & Details
----------- ---------- ------ ------- ----- ----------- ------------------
cucm105pub 10.48.53.190 0.027 Y/Y/Y 0 (g_2) (2) Setup Completed
```

```
cucm105sub1 10.48.53.191 0.292 Y/Y/Y 0 (g_3) (2) Setup Completed
```

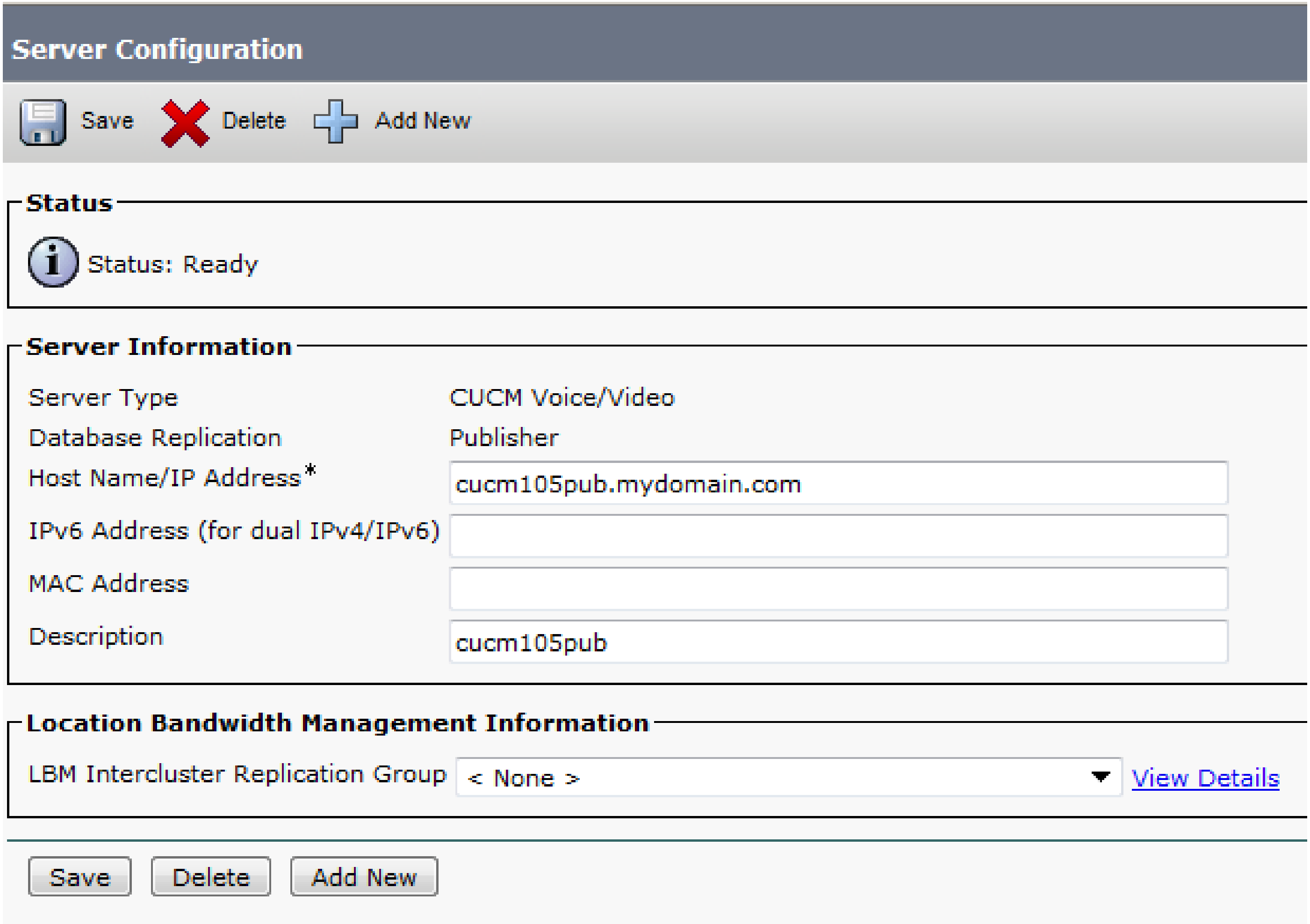
Step 5. Backup.

Run Cisco Disaster Recovery System (DRS) backup of the current setup.

Configuration

Change IP address (or hostname) from IP address to FQDN format in **Cisco Unified CM Administration** web page.

Step 1. Navigate to **System > Server** and change **Host Name/IP Address** field from IP address to FQDN.



Server Configuration

Status

Status: Ready

Server Information

Server Type	CUCM Voice/Video
Database Replication	Publisher
Host Name/IP Address*	cucm105pub.mydomain.com
IPv6 Address (for dual IPv4/IPv6)	
MAC Address	
Description	cucm105pub

Location Bandwidth Management Information

LBM Intercluster Replication Group	< None >

Hostname can be obtained from **show status** and the domain can be obtained from **show network eth0** command output.

Step 2. Repeat the step 1 for for all CUCM servers listed.

Step 3. In order to update configuration files, restart Cisco TFTP service on all CUCM nodes.

Step 4. In order to push updated configuration files to the registered devides, restart Cisco Callmanager service on all CUCM nodes.

Verify

Ensure that all the endpoints successfully registered back with CUCM nodes.

This can be achieved with Real-Time Monitoring Tool (RTMT) help.

In case there is an integration with other servers via SIP, SCCP, MGCP protocols - some configuration might be required on the 3rd party servers.

Ensure that the change is propagated successfully to all the nodes in the CUCM cluster and the output is the same across all nodes.

Execute this command on all the nodes.

```
admin:run sql select name,nodeid from processnode
name nodeid
======================== ======
EnterpriseWideData 1
cucm105pub.mydomain.com 2
cucm105sub1.mydomain.com 3
imp105.mydomain.com 7
```

Related Information

- Troubleshooting CUCM Database Replication in Linux Appliance Model