

Cambiar la definición de servidor CUCM de dirección IP o nombre de host al formato FQDN

Contenido

[Introducción](#)

[Background](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Procedimiento](#)

[Tareas previas al cambio](#)

[Configuración](#)

[Verificación](#)

[Información Relacionada](#)

Introducción

Este documento describe un procedimiento para cambiar la definición del clúster de Cisco Unified Communications Manager (CUCM) de un formato de dirección IP o nombre de host a un formato de nombre de dominio completo (FQDN).

Background

CUCM tiene la opción de elegir si utilizar direcciones IP o servicio de nombres de dominio (DNS) para comunicarse entre nodos y con terminales.

Para los sistemas anteriores a 10.x, la recomendación era no utilizar la dependencia de DNS a menos que se lo requiera un diseño o requisitos específicos.

A partir de CUCM 10.x, debido a la estrecha integración entre CUCM y Cisco Unified Communications Manager IM & Presence Service (IM&P), esa recomendación ha cambiado. Aunque no se puede utilizar DNS en implementaciones básicas de telefonía IP, el uso de nombres de dominio completos en lugar de direcciones IP se convirtió en un requisito para que algunas funciones clave funcionen:

- Inicio de sesión único (SSO)
- Implementaciones de Jabber que requieren el registro del usuario y la detección automática
- Seguridad basada en certificados para medios y señalización seguros

Para configurar una conexión segura, un cliente necesita verificar la identidad del servidor que presenta el certificado.

El cliente realiza la validación en dos pasos:

- En el primer paso, el cliente verifica si el certificado del servidor es de confianza al buscar en su almacén de confianza. Si este certificado de identidad o un certificado de autoridad

certificadora, que se utilizó para firmar el certificado de identidad, está presente en el almacén de confianza del cliente, el certificado se considera de confianza.

- En el segundo paso, el cliente verifica la identidad del servidor en el certificado con respecto a la identidad del servidor en la configuración del cliente local. En otras palabras, el cliente verifica que el nombre del servidor en el certificado y la solicitud de conexión es la misma.

La identidad del servidor en el certificado deriva del atributo Common Name (CN) o del atributo Subject Alternative Name (SAN) del certificado recibido.

Nota: SAN, si está presente, tiene prioridad sobre CN.

La identidad del servidor en la configuración local se deriva del archivo de configuración del dispositivo descargado a través del protocolo trivial de transferencia de archivos (TFTP) y/o de las interacciones de los servicios de datos del usuario (UDS). Los servicios TFTP y UDS derivan esta configuración de la tabla **processnode** de la base de datos. Se puede configurar en la página web **CM Administration > System > Server**.

No confunda la página **CM Administration > System > Server**, donde se definen los servidores, con **OS Administration > Settings > IP Ethernet**, donde se configuran los parámetros de red para los servidores. Los parámetros de la página **OS Administration** afectan a la configuración de red real del servidor; el cambio de nombre de host o dominio lleva a la regeneración de todos los certificados para el nodo. La configuración de la página de administración de CM define, cómo CUCM se anuncia a los terminales a través de archivos de configuración o UDS. El cambio de esta configuración no requiere la regeneración de certificados. Esta configuración debe coincidir con uno de los siguientes parámetros de red del nodo: Dirección IP, nombre de host o FQDN.

Por ejemplo, el terminal se conecta de forma segura a `server.mydomain.com`. Examina el certificado recibido y verifica si "`server.mydomain.com`" está presente en este certificado como CN o SAN. Si la comprobación no se realiza correctamente, la conexión falla o un usuario final recibe un mensaje emergente, solicitando aceptar un certificado no confiable, dependiendo de la funcionalidad del cliente. Dado que los CN y SAN en los certificados normalmente tienen formato FQDN, debe cambiar la definición de servidor de la dirección IP al formato FQDN, si desea evitar estas ventanas emergentes o fallas de conexión.

Prerequisites

Requirements

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CUCM 10.X o superior

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.

Procedimiento

Tareas previas al cambio

Antes de la configuración, se recomienda encarecidamente asegurarse de que se cumplen los requisitos previos.

Paso 1. Verifique la configuración de DNS.

Ejecute estos comandos desde CUCM CLI para asegurarse de que el servicio DNS esté configurado y de que las entradas FQDN para los nombres de nodo se puedan resolver tanto local como externamente.

```
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:
```

Paso 2. Prueba de diagnóstico de red.

Asegúrese de que la prueba de diagnóstico de red se supere ejecutando este comando CLI.

```
admin:utils diagnose module validate_network
```

```
Log file: platform/log/diag3.log
```

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

```
Diagnostics Completed
```

Paso 3. Configuración DHCP para terminales.

Asegúrese de que se agrega la configuración del protocolo de configuración dinámica de host (DHCP) necesaria para que los teléfonos registrados puedan resolver el problema de DNS.

Paso 4. Replicación de la base de datos.

Asegúrese de que la replicación de la base de datos de CUCM funcione. El estado de replicación del clúster debe ser **2** para todos los nodos.

```
admin:utils dbreplication runtimestate
<output omitted for brevity>
Cluster Detailed View from cucml05pub (2 Servers):
  PING DB/RPC/ REPL. Replication REPLICATION SETUP
SERVER-NAME IP ADDRESS (msec) DbMon? QUEUE Group ID (RTMT) & Details
-----
cucml05pub 10.48.53.190 0.027 Y/Y/Y 0 (g_2) (2) Setup Completed
cucml05sub1 10.48.53.191 0.292 Y/Y/Y 0 (g_3) (2) Setup Completed
```

Paso 5. Copia de seguridad.

Ejecute la copia de seguridad del sistema de recuperación ante desastres (DRS) de Cisco de la configuración actual.

Configuración


Cambie la dirección IP (o nombre de host) de la dirección IP al formato FQDN en la página web **Administración de Cisco Unified CM**.

Paso 1. Navegue hasta **System > Server** y cambie el campo **Host Name/IP Address** de la dirección IP a FQDN.

Server Configuration

 Save  Delete  Add New

Status

 Status: Ready

Server Information

Server Type	CUCM Voice/Video
Database Replication	Publisher
Host Name/IP Address*	<input type="text" value="cucm105pub.mydomain.com"/>
IPv6 Address (for dual IPv4/IPv6)	<input type="text"/>
MAC Address	<input type="text"/>
Description	<input type="text" value="cucm105pub"/>

Location Bandwidth Management Information

LBM Intercluster Replication Group [View Details](#)

El nombre de host se puede obtener de **show status** y el dominio se puede obtener de la salida del comando **show network eth0**.

Paso 2. Repita el paso 1 para todos los servidores CUCM enumerados.

Paso 3. Para actualizar los archivos de configuración, reinicie el servicio Cisco TFTP en todos los nodos CUCM.

Paso 4. Para enviar archivos de configuración actualizados a los dispositivos registrados, reinicie el servicio Cisco Callmanager en todos los nodos CUCM.

Verificación

Asegúrese de que todos los terminales se hayan registrado correctamente con los nodos CUCM.

Esto se puede lograr con la ayuda de la herramienta de supervisión en tiempo real (RTMT).

En caso de que exista una integración con otros servidores a través de los protocolos SIP, SCCP y MGCP, es posible que se requiera alguna configuración en los servidores de terceros.

Asegúrese de que el cambio se propague correctamente a todos los nodos del clúster de CUCM y que el resultado sea el mismo en todos los nodos.

Ejecute este comando en todos los nodos.

```
admin:run sql select name,nodeid from processnode
name nodeid
=====
EnterpriseWideData 1
cucml05pub.mydomain.com 2
cucml05sub1.mydomain.com 3
imp105.mydomain.com 7
```

Información Relacionada

- [Solución de problemas de replicación de bases de datos de CUCM en el modelo de dispositivo Linux](#)