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

Contenido

Introducción

Este documento describe un procedimiento cómo cambiar la definición del cluster del administrador de las Comunicaciones unificadas de Cisco (CUCM) de la dirección IP o del formato del nombre de host a un formato del nombre de dominio completo (FQDN).

Antecedente

CUCM tiene una opción a elegir si utilizar los IP Addresses o el servicio de nombre del dominio (DNS) para comunicar entre los Nodos y con los puntos finales.

Para los sistemas pre-10.x la recomendación no era utilizar la confianza DNS a menos que sea requerida por el diseño o los requisitos específicos.

A partir de CUCM 10.x debido a la integración apretada entre CUCM y el administrador de las Comunicaciones unificadas de Cisco IM y servicio de la presencia (IM&P) que la recomendación ha cambiado. Mientras que no usando el DNS en la Telefonía IP básica las implementaciones son todavía aceptables, el uso de los nombres de dominio completamente calificado en vez de los IP Addresses se convirtió en un requisito para que algunas características fundamentales trabajen:

- Escoja Muestra-en (el SSO)
- Farfulle las implementaciones que requieren la detección automática de la inscripción de usuario
- La Seguridad basada en el certificado para asegura la señalización y los media

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 marca si el certificado de servidor es confiado en mirando en su almacén de la confianza. Si este certificado de identidad o un certificado del Certificate Authority, que fue utilizado para firmar el certificado de identidad, está presente en el almacén de la confianza del cliente, el certificado se considera como de confianza.
- En el segundo paso el cliente marca el idenitity del servidor en el certificado contra la identidad del servidor en configuración de cliente local. Es decir el cliente verifica eso Nombre del servidor en el certificado y el pedido de conexión es lo mismo.

La identidad del servidor en el certificado se deriva del atributo del Common Name (CN) o del atributo alternativo sujeto del nombre (SAN) del certificado recibido.

Nota: El SAN, si presente, toma la precedencia sobre el CN.

La identidad del servidor en configuración local se deriva del archivo de configuración del dispositivo descargado vía el Trivial File Transfer Protocol (TFTP) y/o de las interacciones de los servicios de datos del usuario (UD). Los servicios TFTP y UD derivan esta configuración de la tabla del **processnode de la** base de datos. Puede ser configurada en la página web de la **administración >** del **System (Sistema) > Server (Servidor) CM**.

No confunda la página de la administración > del System (Sistema) > Server (Servidor) CM, donde los servidores se están definiendo, con la administración OS > las configuraciones > los Ethernetes IP, donde los parámetros de red para los servidores se están configurando. Parámetros en la configuración de red real de la influencia de la página de administración OS del servidor; el nombre de host o el cambio del dominio lleva a la regeneración de todos los Certificados para el nodo. Las configuraciones en la página de administración CM definen, cómo CUCM se hace publicidad a los puntos finales vía los archivos de configuración o los UD. El cambio de esta configuración no requiere la regeneración de los Certificados. Esta configuración debe hacer juego uno de los parámetros de red siguientes del nodo: Dirección IP, nombre de host o FQDN.

Por ejemplo, su punto final conecta con seguridad con server.mydomain.com. Mira el certificado recibido y lo verifica si “server.mydomail.com” está presente en este certificado como el CN o SAN. Si el control no tiene éxito, la conexión o falla o un usuario final consigue los mensajes emergentes, pidiendo validar el certificado untrusted, dependiendo de la funcionalidad del cliente. Puesto que los CN y sin en los Certificados tienen típicamente formato FQDN, usted necesita cambiar la definición del servidor de la dirección IP al formato FQDN, si usted quiere evitar este popups o fallas de conexión.

Prerrequisitos

Requisitos

Componentes Utilizados

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

- CUCM 10.X o más arriba

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Procedimiento

Tareas del PRE-cambio

Antes de que la configuración él se recomiende altamente para asegurarse de que los requisitos previos están resueltos.

Paso 1. Configuración de DNS del control.

Funcione con estos comandos de CUCM CLI de asegurarse de que el servicio DNS está configurado y las entradas FQDN para los Nombres del nodo se puede resolver localmente y 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 sea pasada funcionando con 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 los puntos finales.

Asegúrese de que la configuración necesaria del Protocolo de configuración dinámica de host (DHCP) esté agregada para que los teléfonos registradoes puedan hacer la resolución de DNS.

Paso 4. Réplica de base de datos.

Asegúrese de que la réplica de base de datos CUCM esté trabajando. El estado de la replicación del cluster debe ser **2** para todos los Nodos.

```
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
```

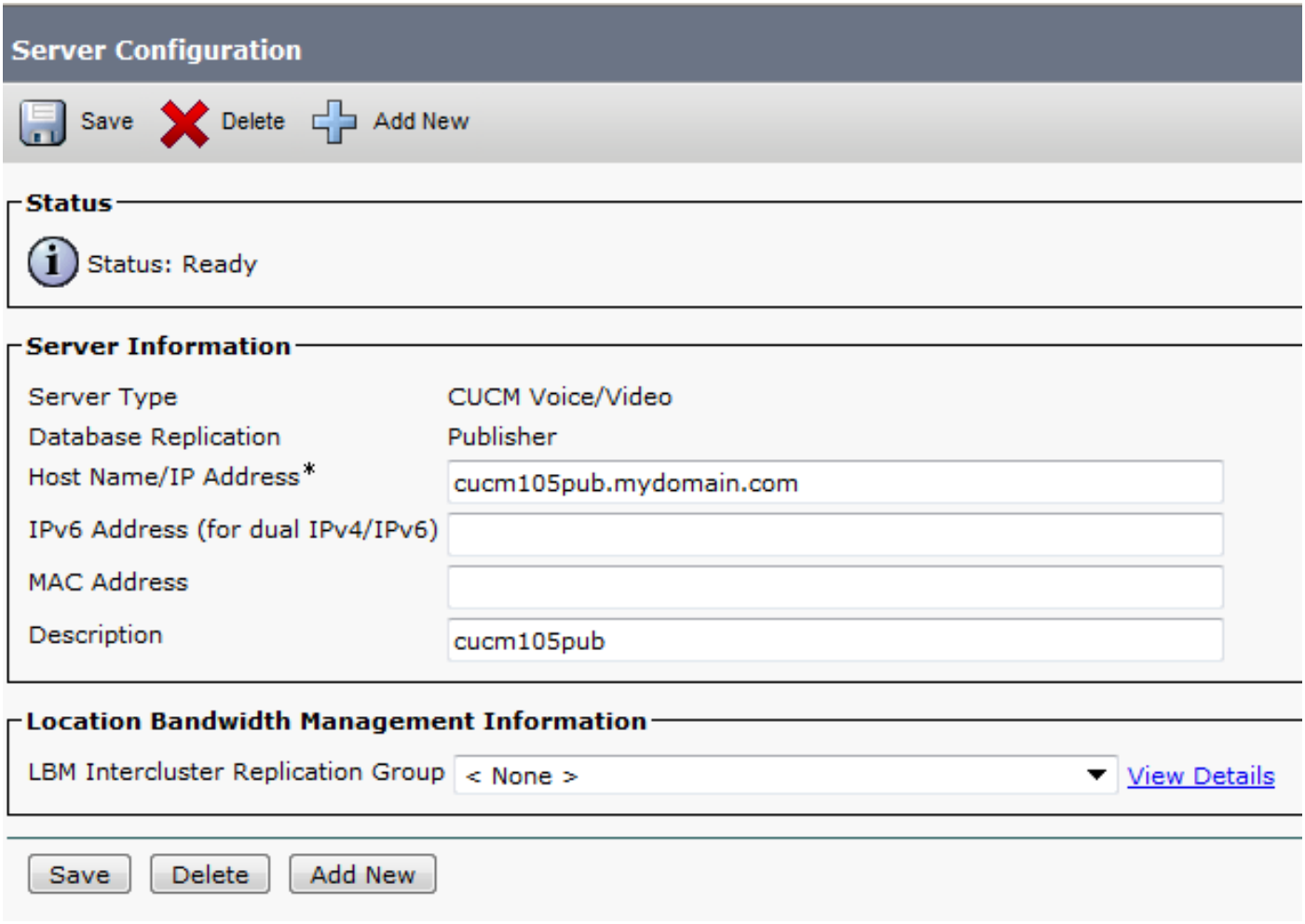
Paso 5. Respaldo.

Funcione con el respaldo del sistema de la Recuperación tras desastres de Cisco (DR) de la configuración actual.

Configuración

Cambie la dirección IP (o el nombre de host) de la dirección IP al formato FQDN en **Cisco unificó la página Web de administración CM**.

Paso 1. Navegue al **System (Sistema) > Server (Servidor)** y cambie el campo del **nombre del host/de la dirección IP de la** dirección IP al FQDN.



El nombre de host se puede obtener del **estatus de la demostración** y el dominio se puede obtener de la salida de comando del **eth0 de la red de la demostración**.

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

Paso 3. Para poner al día los archivos de configuración, reinicio Cisco servicio TFTP en todos los Nodos CUCM.

Paso 4. Para avanzar los archivos de configuración actualizados a los devides registradoes, servicio CallManager de Cisco del reinicio en todos los Nodos CUCM.

Verificación

Asegúrese de que todos los puntos finales se registraran con éxito detrás con los Nodos CUCM.

Esto se puede alcanzar con la ayuda de la herramienta del monitoreo en tiempo real (RTMT).

En caso de que haya una integración con otros servidores vía el SORBO, SCCP, los protocolos MGCP - una cierta configuración se pudo requerir en los servidores de las de otras compañías.

Asegúrese de que el cambio esté propagado con éxito a todos los Nodos en el cluster CUCM y la salida es lo mismo a través de todos los Nodos.

Ejecute este comando en todos los Nodos.

```
admin:run sql select name,nodeid from processnode
```

```
name nodeid
====================== ======
EnterpriseWideData 1
cucm105pub.mydomain.com 2
cucm105sub1.mydomain.com 3
imp105.mydomain.com 7
```

Información Relacionada

- Resolver problemas la réplica de base de datos CUCM en el modelo del dispositivo de Linux