

Modifier la définition du serveur CUCM de l'adresse IP ou du nom d'hôte au format FQDN

Contenu

[Introduction](#)

[Fond](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Procédure](#)

[Tâches de pré-modification](#)

[Configuration](#)

[Vérification](#)

[Informations connexes](#)

Introduction

Ce document décrit une procédure permettant de modifier la définition du cluster Cisco Unified Communications Manager (CUCM) à partir d'une adresse IP ou d'un format de nom d'hôte au format FQDN (Fully Qualified Domain Name).

Fond

CUCM a la possibilité de choisir d'utiliser des adresses IP ou le service DNS (Domain Name Service) afin de communiquer entre les noeuds et avec les points de terminaison.

Pour les systèmes pré-10.x, la recommandation était de ne pas utiliser la dépendance DNS à moins qu'elle ne soit requise par une conception ou des exigences spécifiques.

À partir de CUCM 10.x en raison d'une intégration étroite entre CUCM et Cisco Unified Communications Manager IM & Presence Service (IM&P), cette recommandation a été modifiée. Bien qu'il soit toujours acceptable de ne pas utiliser DNS dans les déploiements de téléphonie IP de base, l'utilisation de noms de domaine complets au lieu d'adresses IP est devenue une exigence pour certaines fonctionnalités clés :

- Authentification unique (SSO)
- Déploiements Jabber nécessitant une détection automatique de l'enregistrement des utilisateurs
- Sécurité basée sur des certificats pour la signalisation et les supports sécurisés

Pour configurer une connexion sécurisée, un client doit vérifier l'identité du serveur qui présente le certificat.

Le client effectue la validation en deux étapes :

- À la première étape, le client vérifie si le certificat du serveur est approuvé en consultant son

magasin de confiance. Si ce certificat d'identité ou un certificat d'autorité de certification, qui a été utilisé pour signer le certificat d'identité, est présent dans le magasin d'approbation du client, le certificat est considéré comme approuvé.

- À la deuxième étape, le client vérifie l'identité du serveur dans le certificat par rapport à celle du serveur dans la configuration du client local. En d'autres termes, le client vérifie que le nom du serveur dans le certificat et la demande de connexion sont identiques.

L'identité du serveur dans le certificat est dérivée de l'attribut Common Name Attribute (CN) ou Subject Alternative Name (SAN) du certificat reçu.

Note: Le SAN, s'il est présent, a préséance sur le CN.

L'identité du serveur dans la configuration locale provient du fichier de configuration de périphérique téléchargé via TFTP (Trivial File Transfer Protocol) et/ou des interactions UDS (User Data Services). Les services TFTP et UDS dérivent cette configuration de la table de **noeud de traitement de** base de données. Il peut être configuré dans la page Web **Administration CM > Système > Serveur**.

Ne confondez pas CM Administration > System > Server page, où les serveurs sont définis, avec OS Administration > Settings > IP Ethernet, où les paramètres réseau des serveurs sont configurés. Les paramètres de la page Administration du système d'exploitation affectent la configuration réseau réelle du serveur ; le changement de nom d'hôte ou de domaine entraîne la régénération de tous les certificats pour le noeud. Les paramètres de la page Administration de CM définissent la façon dont CUCM s'annonce aux points de terminaison via des fichiers de configuration ou UDS. La modification de ce paramètre ne nécessite pas la régénération des certificats. Ce paramètre doit correspondre à l'un des paramètres réseau suivants du noeud : Adresse IP, nom d'hôte ou nom de domaine complet (FQDN).

Par exemple, votre terminal se connecte en toute sécurité à server.mydomain.com. Il examine le certificat reçu et vérifie si « server.mydomain.com » est présent dans ce certificat en tant que CN ou SAN. Si la vérification échoue, la connexion échoue ou un utilisateur final reçoit un message contextuel, lui demandant d'accepter un certificat non approuvé, selon la fonctionnalité du client. Puisque les CN et les SAN des certificats ont généralement un format FQDN, vous devez modifier la définition du serveur de l'adresse IP au format FQDN, si vous voulez éviter ces fenêtres publicitaires intempestives ou ces échecs de connexion.

Conditions préalables

Conditions requises

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CUCM 10.X ou supérieur

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.

Procédure

Tâches de pré-modification

Avant la configuration, il est fortement recommandé de s'assurer que les conditions requises sont remplies.

Étape 1. Vérifiez la configuration DNS.

Exécutez ces commandes à partir de l'interface de ligne de commande de CUCM pour vous assurer que le service DNS est configuré et que les entrées FQDN pour les noms de noeud peuvent être résolues localement et en externe.

```
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:
```

Étape 2. Test de diagnostic du réseau.

Assurez-vous que le test de diagnostic réseau est réussi en exécutant cette commande CLI.

```
admin:utils diagnose module validate_network

Log file: platform/log/diag3.log

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

Diagnostics Completed
```

Étape 3. Configuration DHCP pour les points de terminaison.

Assurez-vous que la configuration Dynamic Host Configuration Protocol (DHCP) nécessaire est

ajoutée pour que les téléphones enregistrés puissent effectuer la résolution DNS.

Étape 4. Réplication de base de données.

Assurez-vous que la réplication de base de données CUCM fonctionne. L'état de réplication du cluster doit être **2** pour tous les noeuds.

```
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
```

Étape 5. Sauvegarde.




Exécutez la sauvegarde Cisco Disaster Recovery System (DRS) de la configuration actuelle.

Configuration


Modifiez l'adresse IP (ou le nom d'hôte) de l'adresse IP au format FQDN dans la page Web **Cisco Unified CM Administration**.

Étape 1. Accédez à **System > Server** et modifiez le champ **Host Name/IP Address** de l'adresse IP au nom de domaine complet.

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](#)

Save Delete Add New

Le nom d'hôte peut être obtenu à partir de **show status** et le domaine peut être obtenu à partir de la sortie de commande **show network eth0**.

Étape 2. Répétez l'étape 1 pour tous les serveurs CUCM répertoriés.

Étape 3. Afin de mettre à jour les fichiers de configuration, redémarrez le service TFTP de Cisco sur tous les noeuds CUCM.

Étape 4. Afin de transmettre les fichiers de configuration mis à jour aux périphériques enregistrés, redémarrez le service Cisco Callmanager sur tous les noeuds CUCM.

Vérification

Assurez-vous que tous les points de terminaison ont été enregistrés avec succès avec les noeuds CUCM.

Cela peut être réalisé avec l'aide de l'outil de surveillance en temps réel (RTMT).

En cas d'intégration avec d'autres serveurs via les protocoles SIP, SCCP et MGCP, une configuration peut être requise sur les serveurs tiers.

Assurez-vous que la modification est propagée correctement à tous les noeuds du cluster CUCM et que le résultat est le même sur tous les noeuds.

Exécutez cette commande sur tous les noeuds.

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

Informations connexes

- [Dépannage de la réplication de base de données CUCM dans le modèle d'appliance Linux](#)