Installation unifiée de batterie de transmission avec l'exemple soumis multiserveur Ca-signé de configuration de nom secondaire

Contenu

Introduction

Ce document décrit comment installer une batterie unifiée de transmission avec l'utilisation d'un Autorité de certification (CA) - le nom secondaire soumis multiserveur signé (SAN).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Communications Manager (CUCM)
- CUCM IM et version 10.5 de présence

Avant que vous tentiez cette configuration, assurez que ces services sont hauts et fonctionnels :

- Service Web administratif de plate-forme de Cisco
- Service de Cisco Tomcat

Afin de vérifier ces services sur une interface web, naviguez vers des **services > le service réseau de page d'utilité de Cisco Unified > sélectionnent un serveur**. Afin de les vérifier sur le CLI, sélectionnez la commande de **liste de service d'utils**.

[Composants utilisés](#)

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Dans la version 10.5 et ultérieures CUCM, cette demande de la demande de signature de certificat de confiance-mémoire (CSR) peut inclure le SAN et les domaines alternatifs.

1. Tomcat
2. Cisco CallManager (CCM)
3. Messagerie et présence Présence-extensibles Protocol (CUP-XMPP) de Cisco Unified
4. Serveur-à-serveur CUP-XMPP (S2S)

Il est plus simple d'obtenir un certificat Ca-signé dans cette version. Seulement un CSR est exigé pour être signé par CA plutôt que la condition requise d'obtenir un CSR de chaque noeud de serveur et puis d'obtenir un certificat Ca-signé pour chaque CSR et de les gérer individuellement.

Configurez

1. Connectez-vous dans la gestion du système d'exploitation (de SYSTÈME D'EXPLOITATION) et naviguez vers la **Gestion de Sécurité > de certificat > génèrent le CSR**.

2. **SAN multiserveur** choisi dans la distribution.

   Il autopopulates les domaines SAN et le domaine de parent.

   Une fois qu'il est généré, ceci affiche :

   En Gestion de certificat, la demande SAN est générée :

3. Vous pouvez utiliser les gens du pays CA ou un CA externe comme Verisign afin de l'obtenir a signé. Cet exemple affiche des étapes de configuration pour Microsoft Windows CA basé

sur un serveur.

Connectez-vous dans https:// <windowsserveripaddress>/certsrv/

La demande choisie un **certificat > a avancé la demande de certificat**.

4. Soumettez la demande CSR comme affiché ici.

5. Une fois que vous obtenez le certificat, vous devez télécharger le certificat de CA pendant que Tomcat-confiance et puis téléchargez le certificat Ca-signé comme chat.

6. Assurez que le service est redémarré sur tous les Noeuds dans la liste SAN, qui inclut le noeud où elle est téléchargée. Vous voyez le SAN multiserveur répertorié en Gestion de certificat.

Vérifiez

Connectez-vous dans http://<fqdnofccm>:8443/ccmadmin afin de s'assurer que le nouveau certificat est utilisé.

Certificat multiserveur du CallManager SAN

Une procédure semblable peut être suivie pour le certificat de CallManager. Dans ce cas, les domaines autopopulated sont tous les Noeuds de CallManager. S'il ne fonctionne pas, vous pouvez choisir de le garder de la liste SAN ou de le retirer de là.

Après que vous installiez le certificat délivré par CA, vous devez redémarrer le service de CallManager sur tous les Noeuds.

Avant que vous obteniez le certificat Ca-signé SAN pour CUCM, assurez cela :

- Le téléphone IP peut faire confiance au service de vérification de confiance (TV). Ceci peut être vérifié si vous accédez à n'importe quel service HTTPS du téléphone. Par exemple, si l'accès de répertoire d'entreprise fonctionne, puis il signifie que le téléphone fait confiance au service TV.
- Si c'est une batterie sécurisée, assurez-vous que le client de la liste de confiance de certificat (CTL) est réexécuté de sorte qu'un nouveau fichier CTL est créé et la batterie est redémarrée.

Dépannez

Ces logs devraient aider le centre d'assistance technique Cisco à identifier n'importe quel problème lié à la génération CSR SAN et au téléchargement multiserveurs Ca-Signer Certficate.

- Plate-forme API de SYSTÈME D'EXPLOITATION de Cisco Unified
- Cisco Tomcat
- Logs de CertMgr de plate-forme IPT

Dans un Certifcate multiserveur existant CUCM, si l'adresse Internet du serveur change, il est recommandé pour générer une demande multiserveuse CSR SAN comme expliqué précédemment afin d'obtenir le certificat signé par CA.