Renouveler le certificat Expressway

Contenu

Introduction

Ce document décrit le processus de renouvellement de certificat d'Expressway/Video Communication Server (VCS).

Les informations contenues dans ce document s'appliquent à Expressway et à VCS. Le document fait référence à Expressway mais il peut être échangé avec VCS.

> **Note**: Bien que ce document soit conçu pour vous aider dans le processus de renouvellement des certificats, il est conseillé de consulter également le Guide de création et d'utilisation des certificats Cisco Expressway pour votre version.

Informations générales

Lors du renouvellement d'un certificat, deux points principaux doivent être pris en compte pour s'assurer que le système continue à fonctionner correctement une fois le nouveau certificat installé :

1. Les attributs du nouveau certificat doivent correspondre à ceux de l'ancien certificat (principalement le nom secondaire du sujet et l'utilisation de la clé étendue)

2. L'autorité de certification (CA) à utiliser pour signer le nouveau certificat doit être approuvée par d'autres serveurs qui communiquent directement avec l'Expressway (par exemple CUCM, Expressway-C, Expressway-E..etc)

Process

A) Obtenir des informations du certificat actuel

1. Ouvrez la page Web Expressway **Maintenance > Security > Server certificate > Show decoded.**

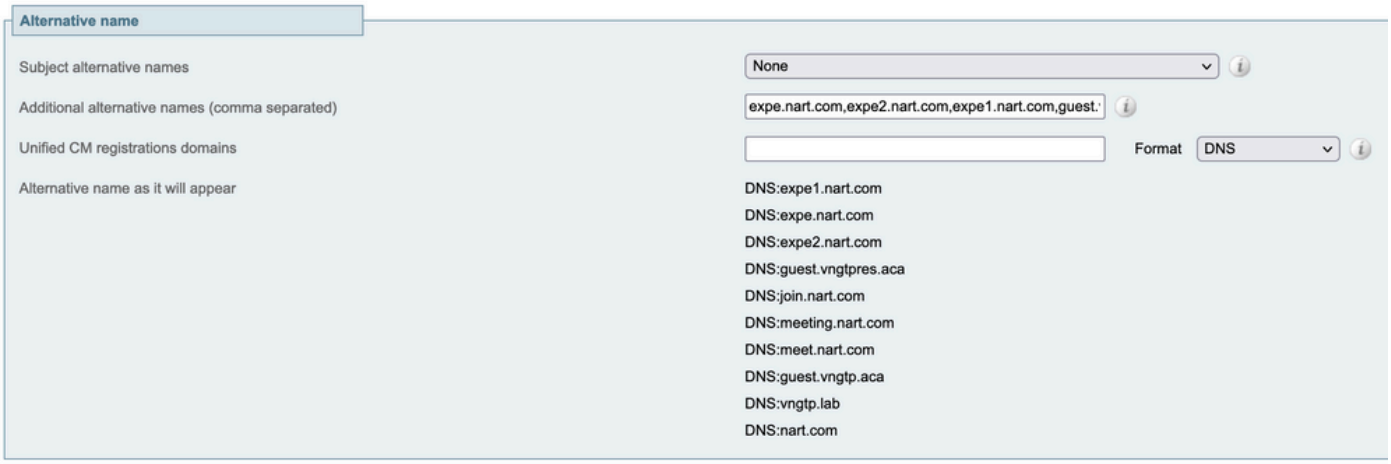
2. Dans la nouvelle fenêtre qui s'ouvre, copiez les extensions X509v3 « Subject Alternative name » et « Authority Key Identifier » dans un document de bloc-notes.

Fenêtre de certificat « Show decoded »

B) Générez la demande de signature de certificat (CSR) et envoyez-la à l'autorité de certification (CA) pour signature.

1. Depuis la page Web Expressway **Maintenance > Security > Server certificate > Generate CSR.**

2. Dans la fenêtre Generate CSR, dans le champ **Additional alternative names (virgules séparées)**, renseignez toutes les valeurs pour "Subject Alternative Names" que nous avons enregistrées dans la section A, et assurez-vous de supprimer "DNS :" et séparez la liste par des virgules, voir image (à côté de "Alternative name as it will look", vous pouvez voir une liste de tous les SAN à utiliser dans le certificat) :



Générer des entrées SAN CSR

3. Remplissez le reste des informations sous la section **Informations supplémentaires** telles que le pays, la société, l'état... et cliquez sur **Générer CSR.**

4. Une fois que vous avez généré le CSR, la page **Maintenance > Security > Server Certificate** affiche une option pour **Discard CSR** and **Download**, vous devez choisir **Download** et envoyer le CSR à l'autorité de certification pour signature.

> **Note**: Assurez-vous de ne pas **Rejeter CSR** avant que le nouveau certificat soit installé, si **Rejeter CSR** a été fait et qu'une tentative d'installation d'un certificat signé avec le CSR qui a été rejeté, l'installation du certificat échoue.

C) Vérifiez la liste SAN et l'attribut d'utilisation de clé étendue/améliorée dans le nouveau certificat

Ouvrez le certificat nouvellement signé dans le gestionnaire de certificats Windows et recherchez :

1. La liste SAN correspond à la liste SAN que nous avons enregistrée dans la section A que nous

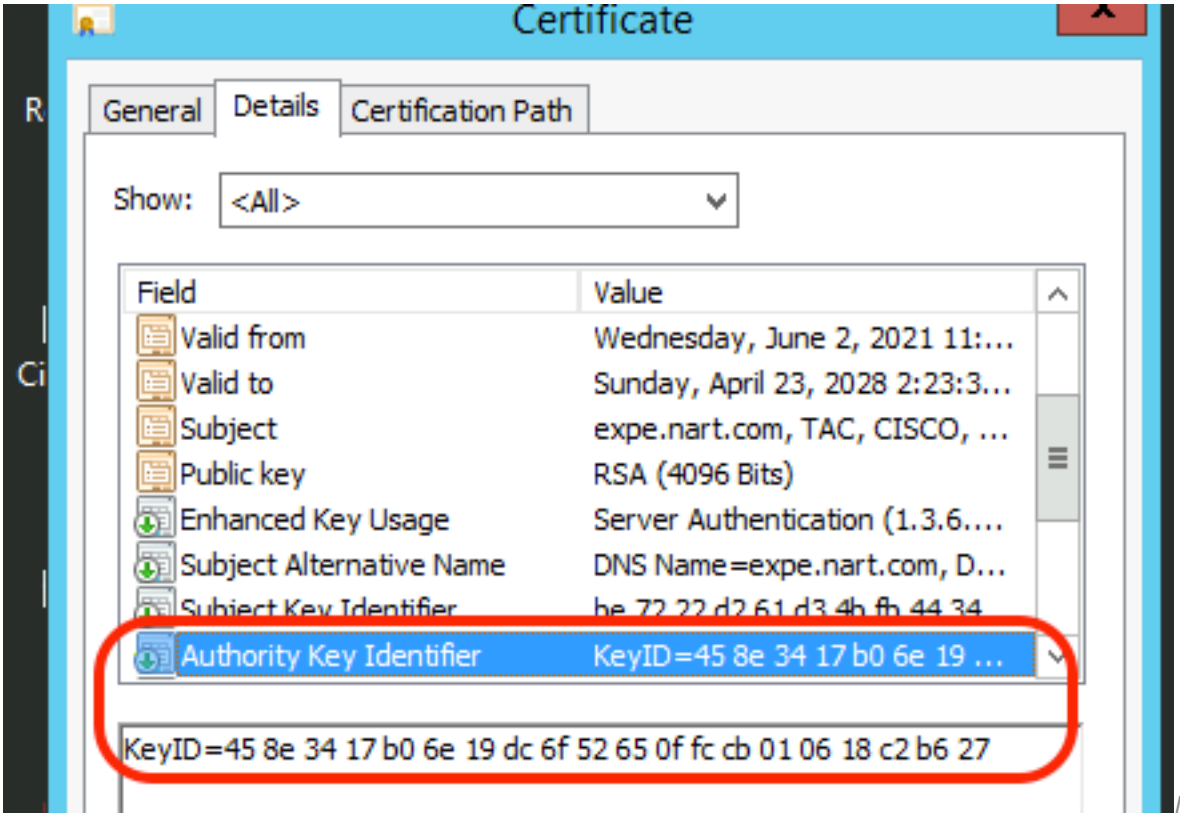
avons utilisée pour générer le CSR.

2. L'attribut « Extended/Enhanced key usage » doit inclure « Client Authentication » et « Server Authentication ».

> **Note**: Si le certificat a l'extension .pem, renommez-le en .cer ou .crt pour pouvoir l'ouvrir avec le Gestionnaire de certificats Windows. Une fois le certificat ouvert avec le Gestionnaire de certificats Windows, vous pouvez aller à l'onglet **Détails > Copier dans fichier** et l'exporter en tant que fichier codé en Base64, un fichier codé en Base64 a normalement "-----BEGIN CERTIFICATE-----" en haut et "-----END CERTIFICATE-----" en bas lorsqu'il est ouvert dans un éditeur de texte

D) Vérifiez si l'autorité de certification qui a signé le nouveau certificat est la même que celle qui a signé l'ancien certificat

Ouvrez le certificat nouvellement signé dans le gestionnaire de certificats Windows et copiez la valeur « Identificateur de clé d'autorité » et comparez-la à la valeur « Identificateur de clé d'autorité » que nous avons enregistrée dans la section A.



Nouveau certificat ouvert avec le Gestionnaire de certificats Windows

Si les deux valeurs sont identiques, cela signifie que la même autorité de certification a été utilisée pour signer le nouveau certificat que celle qui a été utilisée pour signer l'ancien certificat, et vous pouvez passer à la section E pour télécharger le nouveau certificat.

Si les valeurs sont différentes, cela signifie que l'autorité de certification utilisée pour signer le nouveau certificat est différente de celle utilisée pour signer l'ancien certificat, et les étapes à suivre avant de pouvoir passer à la section E sont les suivantes :

1. Obtenez tous les certificats d'autorité de certification intermédiaire (le cas échéant) et le certificat d'autorité de certification racine.

2. Allez à **Maintenance > Security > Trusted CA certificate** , cliquez sur **Browse** puis recherchez le certificat intermédiaire de l'autorité de certification sur votre ordinateur et téléchargez-le. Faites de même pour les autres certificats d'autorité de certification intermédiaires et le certificat d'autorité de certification racine.

3. Procédez de la même manière sur tout Expressway-E (si le certificat à renouveler est un certificat Expressway-C) qui se connecte à ce serveur ou tout Expressway-C (si le certificat à renouveler est un certificat Expressway-E) qui se connecte à ce serveur.

4. Si le certificat à renouveler est un certificat Expressway-C et que vous disposez d'un MRA ou de zones sécurisées pour CUCM, vous devez vous assurer que CUCM approuve la nouvelle autorité de certification racine et intermédiaire et télécharger les certificats d'autorité de certification racine et intermédiaire vers les magasins CUCM tomcat-trust et callmanager-trust, puis redémarrer les services appropriés sur CUCM.

E) Installer le nouveau certificat

Une fois que tous les points précédents ont été vérifiés, vous pouvez maintenant installer le nouveau certificat sur l'Expressway à partir de **Maintenance > Security > Server Certificate** cliquez sur **Browse** et sélectionnez le nouveau fichier de certificat à partir de votre ordinateur et le télécharger.

Vous devez redémarrer l'Expressway après avoir installé un nouveau certificat.

> **Note**: Assurez-vous que le certificat que vous téléchargez vers Expressway à partir de **Maintenance > Sécurité > Certificat de serveur** contient uniquement le certificat de serveur Expressway et NON la chaîne de certificats complète et assurez-vous que son certificat Base64

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.