Exemple de configuration d'autorité de certification de serveur de communication vidéo

Contenu

Introduction

Ce document décrit l'authentification de certificat sur le serveur de communication vidéo (VCS). Un certificat identifie le VCS et contient les noms par lesquels on le connaît et à quel trafic est conduit. Si le VCS est connu par de plusieurs noms dans ces buts, comme si ce fait partie d'une batterie, ceci doit être représenté dans les données du sujet X.509. Le certificat doit contenir le nom de domaine complet (FQDN) du VCS lui-même et de la batterie. Si un certificat est partagé à travers des pairs de batterie, il doit répertorier tous les FQDN possibles de pair.

UN VCS a besoin des Certificats pour :

- HTTP sécurisé avec la Connectivité de Transport Layer Security (TLS) (HTTPS)
- Connectivité de TLS pour la signalisation de Protocole SIP (Session Initiation Protocol), les points finaux, et les zones voisines
- Connexions à d'autres systèmes tels que des serveurs de Cisco Unified Communications Manager (CUCM), de la suite logicielle de gestion Cisco TelePresence (TMS), du Protocole LDAP (Lightweight Directory Access Protocol), et des serveurs de Syslog

Il emploie sa liste de Certificats de confiance d'Autorité de certification (CA) et de listes des révocations de certificat associées (CRLs) afin de valider d'autres périphériques qui se connectent à elle.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- VCS - Versions 8.1 et 8.1.1
- Autorité de certification - Entreprise R2 de Microsoft Windows 2008

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

La version 8.1.1 de VCS prend en charge la caractéristique mobile de l'Accès à distance de périphérie de Collab (MRA) et exige une connexion de TLS entre le VCS-Control et le VCS-Expressway.

Afin d'installer le TLS, vous devez télécharger les Certificats nécessaires sur le VCS. Vous pouvez se terminer ceci avec ces trois méthodes :

- OpenSSL
- Entreprise CA
- Tierce partie CA

La connexion de TLS entre le VCS-Control et le VCS-Expressway exige ces deux attributs :

- Authentification client de TLS
- Authentification de serveur Web de TLS

Ce document se concentre sur la méthode de l'entreprise CA pendant qu'OpenSSL est déjà discuté dans le guide de déploiement de certificat de VCS.

Quand vous installez le CA, le certificat de web server est livré par défaut. Cependant, ce modèle ne peut pas être utilisé pour générer le certificat pour la connexion de TLS entre le VCS-Control et le VCS-Expressway. Si vous essayez de télécharger le certificat au VCS, qui est généré avec juste l'attribut de web server, vous recevez cette erreur.

Afin de vérifier ceci, **certificat** choisi de **maintenance > de serveur**. Le clic **décodent le certificat**. Vérifiez la section « a étendu l'utilisation principale ».

Configurez

Comme indiqué plus tôt, parce que la connexion de TLS vous avez besoin d'un attribut de client et de web server. Puisqu'il n'y a pas un modèle par défaut, vous pouvez créer un. Terminez-vous ces étapes afin de générer le nouveau modèle avec les attributs d'authentification d'authentification client de TLS et de serveur Web de TLS :

1. Ouvrez l'autorité de certification ou allez à la console de Microsoft Management Console (MMC). Cliquez sur Add**/enlevez l'autorité de certification Snapin** et choisie. Développez le CA dans le volet gauche et sélectionnez les **modèles de certificat**. Cliquez avec le bouton droit le modèle de certificat et choisi **gérez**.
2. Cliquez avec le bouton droit le modèle de certificat de **serveur Web** et sélectionnez le **modèle en double**.
3. Cliquez sur la case d'option **2003 d'entreprise de Windows Server** (si vous voulez que le modèle soit disponible pour l'inscription de Web). Cliquez sur **OK**.
4. Écrivez le nom du modèle dans la zone d'identification d'affichage de modèle. Nommez le modèle selon vos conditions requises, par exemple « client de web server 2003".
5. Cliquez sur l'onglet d'**extensions** et sélectionnez la stratégie d'application. Cliquez sur **Edit**.
6. Dans la boîte de dialogue de stratégie d'application d'ajouter, **authentification client** choisie. Cliquez sur **OK**.
7. Dans la boîte de dialogue d'extension de stratégies d'application d'éditer, cliquez sur OK.
8. De la console MMC ou de la fenêtre CA, **modèle de certificat de** clic droit. Sélectionnez **nouveau > modèle de certificat à émettre**.
9. Sélectionnez votre modèle de création récente dans la boîte de dialogue de modèles de certificat d'enable. Vérifiez le modèle dans la colonne de **but visé**. Cliquez sur **OK**.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Procédez comme suit :

1. Vérifiez que votre modèle demandé de certificat est disponible afin de délivrer de nouveaux Certificats.**Note**: Le modèle sera disponible pour l'inscription de Web seulement si vous sélectionniez le modèle comme Windows 2003 quand vous avez créé le modèle de certificat.
2. Suivez la procédure pour générer la demande de signature de certificat (CSR) du VCS et pour obtenir le certificat signé avec le nouveau modèle.
3. Vérifiez que le certificat a le client et l'attribut de web server disponibles.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Si le modèle n'est pas disponible pour l'inscription de Web, déterminez si l'utilisateur qui accède au **certsrv** a les autorisations nécessaires.

Comme indiqué précédemment, le modèle de Windows 2008 ne sera pas disponible pour l'inscription de Web. Pour plus de détails, voir les modèles de l'inscription 2008 et de la version 3 de Web.