Créer un certificat racine personnalisé Umbrella avec les services de certificats AD

Table des matières

Introduction

Ce document décrit les instructions pour créer un certificat racine personnalisé à l'aide des services de certificats Microsoft Windows Active Directory (AD).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Version de Microsoft Windows Server actuellement prise en charge par Microsoft
- Services de certificats Active Directory installés sur le serveur Windows
- Un compte avec les rôles Services de certificats Active Directory et Service Web/Service d'inscription Web
- Services de certificats configurés pour émettre des certificats avec le codage UTF-8 ("UTF8STRING")

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Cet article contient des instructions pour créer un certificat racine personnalisé (qui est utilisé à la place du certificat CA racine standard de Cisco Umbrella) à l'aide des services de certificats Microsoft Windows Active Directory, puis pour utiliser ce certificat racine pour signer une demande de signature de certificat (CSR) à partir de la fonctionnalité de certificat CA signé par le client d'Umbrella.

Codage de chaîne de certificat

Si vos services de certificats sont configurés pour utiliser le codage par défaut ("PRINTABLESTRING"), la chaîne de certificats produite ne peut pas être approuvée par certains clients Web, en particulier Firefox.

Le proxy Cisco Umbrella Secure Web Gateway utilise une chaîne de certificats qui code les chaînes avec le codage UTF8STRING. Si votre certificat d'émission (par exemple, votre certificat racine) qui signe le CSR pour créer le certificat intermédiaire CA Cisco Umbrella Customers est codé avec PRINTABLESTRING, alors le codage du champ Objet du certificat CA Cisco Umbrella Customers est PRINTABLESTRING. Ce codage ne peut pas correspondre au codage UTF8STRING du champ Issuer dans le certificat intermédiaire de l'autorité de certification Cisco Umbrella R1, qui est le suivant dans la chaîne de certificats.

RFC 5280 La section 4.1.2.6 exige qu'une chaîne de certificats conserve le même codage de chaîne entre le champ Issuer d'un certificat émis et le champ Subject dans le certificat émis :

« Lorsque le sujet du certificat est une AC, le champ sujet DOIT être codé de la même façon que dans le champ émetteur (section 4.1.2.4) dans tous les certificats émis par l'AC sujet. »

De nombreux navigateurs n'appliquent pas cette exigence, mais certains (notamment Firefox) le font. Par conséquent, les clients Web tels que Firefox peuvent générer une erreur de site non fiable et ne pas charger de sites Web lors de l'utilisation de Secure Web Gateway (SWG) avec la fonctionnalité de certificat CA signé par l'autorité de certification du client.

Pour contourner ce problème, utilisez un navigateur tel que Chrome qui n'applique pas les exigences de la RFC 5280.

Étape 1 : Préparation du modèle de services de certificats AD

1. Ouvrez la console MMC de l'autorité de certification Active Directory en sélectionnant Démarrer > Exécuter > MMC.

2. Sélectionnez Fichier > Ajouter/Supprimer un composant logiciel enfichable et ajoutez les composants logiciels enfichables Modèles de certificat et Autorité de certification. Sélectionnez OK.

3. Développez Modèles de certificat et cliquez avec le bouton droit sur Autorité de certification subordonnée. Cliquez sur Modèle dupliqué.

Vous pouvez maintenant créer un modèle de certificat personnalisé pour répondre aux exigences répertoriées dans la documentation Umbrella.

Voici les conditions qui sont détaillées au moment de la création de cet article :

- Onglet Général
  - Donnez au modèle un nom qui a du sens pour vous.
  - Définissez la période de validité de 35 mois (3 ans moins un mois).
  - Définissez la période de renouvellement sur 20 jours.
- onglet Extensions
  - Double-cliquez sur Contraintes de base.
    - Assurez-vous que l'option Rendre ce poste critique est sélectionnée.
  - Sous Utilisation des clés :
    - Assurez-vous que la signature de certificat &la signature CRL sont sélectionnées.
    - Désélectionnez Signature numérique.
    - Assurez-vous que Make this extension critical est également coché ici.
- Sélectionnez Appliquer et OK

Étape 2 : Émettre le modèle

1. Dans la console MMC que vous avez configurée à l'étape 2 du processus précédent, développez la section Autorité de certification.

2. Dans la section nouvellement développée, cliquez avec le bouton droit sur le dossier Certificate Templates et sélectionnez New > Certificate Template to Issue.

3. Dans la nouvelle fenêtre, sélectionnez le nom du modèle de certificat que vous avez créé dans la dernière section et cliquez sur OK.

L'AC est maintenant prête à faciliter la demande.

Étape 3 : Téléchargement et signature du CSR

1. Connectez-vous à votre tableau de bord Umbrella (https://dashboard.umbrella.com).

2. Accédez à Déploiements > Configuration > Root Certificate.

3. Sélectionnez l'icône Ajouter (+) dans le coin et nommez votre autorité de certification dans la nouvelle fenêtre.

4. Téléchargez la demande de signature de certificat (CSR).

5. Dans un nouvel onglet de navigateur, accédez aux services Web pour les services de certificats Active Directory. (Si vous utilisez une machine locale, il s'agit de 127.0.0.1/certsrv/ ou similaire.)

6. Dans la nouvelle page, sélectionnez Demander un certificat.

7. Sélectionnez Demande de certificat avancée.

8. Sous Requête enregistrée, copiez et collez le contenu du CSR que vous avez téléchargé à l'étape 4 (vous devez l'ouvrir avec un éditeur de texte).

9. Sous Modèle de certificat, sélectionnez le nom du modèle de certificat que vous avez créé dans la section "Préparation du modèle de services de certificats AD" et sélectionnez Soumettre.

10. Veillez à sélectionner Base64 Encoded et sélectionnez Download Certificate et notez l'emplacement du fichier .cer.

Étape 4 : Télécharger le CSR signé (et le certificat racine public)

1. Sur votre tableau de bord Umbrella, accédez à Déploiement > Configuration > Certificat racine.

2. Sélectionnez le certificat racine que vous avez créé à l'étape 3 de la section précédente.

3. Sélectionnez Upload CA dans le coin inférieur droit de la ligne*.

4. Sélectionnez le bouton Browse supérieur (Certificate Authority (Signed CSR)).

5. Accédez à l'emplacement du fichier .cer que vous avez créé dans la section précédente et sélectionnez Enregistrer.

6. Sélectionnez Next et sélectionnez les groupes d'ordinateurs/utilisateurs avec lesquels vous souhaitez utiliser le certificat (au lieu du certificat racine Cisco) et sélectionnez Save.

*Vous pouvez également télécharger le certificat CA en option. Vous pouvez le récupérer à partir de l'interface Web de votre serveur d'autorité de certification (http://127.0.0.1/certsrv/), puis en sélectionnant Download a CA Certificate, Certificate Chain, or CRL. Complétez les invites à l'écran pour « Download the CA certificate » (Télécharger le certificat d'autorité de certification) en Base 64.

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.