Contenu

Introduction

Ce document explique comment générer une demande de signature de certificat (CSR) afin d'obtenir un tiers certificat avec un système de contrôle sans fil (WCS) et comment télécharger le certificat sur le WCS.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- La connaissance de la façon installer et configurer WCS pour le fonctionnement de base
- La connaissance d'auto-signé et des Certificats numériques, et d'autres mécanismes de sécurité a associé à l'Infrastructure à clés publiques (PKI)

Composants utilisés

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

- Version 4.1.91.0 WCS**Remarque:** La génération CSR qui utilise un WCS est seulement commencer pris en charge par la version 4.1.91.0 WCS.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Demande de signature de certificat (CSR)

Un certificat est un document électronique que vous employez afin d'identifier un serveur, une société, ou une autre entité et associer cette identité avec une clé publique.

Un certificat auto-signé est un certificat d'identité qui est signé par son propre créateur. C'est-à-dire, la personne qui a créé le certificat également s'est déconnectée sur sa légitimité.

Des Certificats peuvent auto-être signés ou peuvent être certifiés par une signature numérique d'un Autorité de certification (CA).

Les CAs sont des entités qui valident des identités et délivrent des Certificats. Le certificat que le CA fournit des grippages une clé publique particulière au nom de l'entité que le certificat identifie, comme le nom d'un serveur ou d'un périphérique. Seulement la clé publique que le certificat certifie des travaux avec la clé privée correspondante a possédé par l'entité que le certificat identifie. Les Certificats aident à empêcher l'utilisation de fausses clés publiques pour la personnification.

Un CSR est un message qu'un candidat envoie à un CA afin de solliciter un certificat d'identité numérique. Avant qu'un CSR soit créé, le candidat génère d'abord une paire de clés, qui maintient la clé privée secrète. Le CSR contient les informations qui identifient le candidat, tel qu'un nom du répertoire dans le cas d'un certificat X.509, et la clé publique choisie par le candidat. La clé privée correspondante n'est pas incluse dans le CSR, mais est utilisée pour signer digitalement la demande entière.

Le CSR peut être accompagné d'autres qualifications ou preuves d'identité exigées par l'autorité de certification, et l'autorité de certification peut contacter le candidat pour de plus amples informations. Pour la plupart, une société de la tierce partie CA, comme confient ou Verisign, exige un CSR avant que la société puisse créer un certificat numérique.

La génération CSR est indépendant du périphérique sur lequel vous prévoyez d'installer un certificat externe. Par conséquent, un CSR et un fichier principal privé peuvent être générés sur n'importe quel ordinateur individuel qui prend en charge la génération CSR. La génération CSR n'est pas commutateur-dépendante ou appliance-dépendante dans ce cas.

Ce document explique comment générer le CSR pour un tiers certificat utilisant le Cisco WCS.

Génération CSR utilisant un WCS

CSRs sur un WCS peut être généré utilisant un outil disponible dans le répertoire d'installation WCS. Cet outil s'appelle le **keyadmin.bat.**

Remarque: Si le WCS est installé sur le Linux, vous devrez utiliser l'outil de **keyadmin.sh** disponible chez **/opt/WCS4.1/bin/**. Cet exemple affiche comment générer un CSR et importer le certificat signé utilisant un WCS installé sur un serveur de Microsoft Windows 2003. L'utilisateur

de base du WCS doit exécuter cette procédure de sorte que le certificat puisse être généré.

Terminez-vous ces étapes afin d'accéder à l'outil :

1. Allez à l'**invite de commande** disponible avec Windows.
2. Allez le répertoire d'installation WCS, puis au **coffre de** répertoire.Voici un exemple :**C:\CD Program FilesC:\Program Files>CD WCS4.1C:\Program Files\WCS4.1> cd binC:\Program Files\WCS4.1\bin>**Ce répertoire aura l'**outil keyadmin.bat** qui est utilisé pour générer le CSR.
3. Terminez-vous ces étapes afin de générer le CSR :Sélectionnez cette commande :**keyadmin -newdn -csr genkey** [csrFileName]Ceci génère une nouvelle clé/paire auto-signée de certificat, et a sorti le CSR au fichier spécifié. **- L'**indicateur de **newdn** le fait inciter pour les champs de nom unique pour le certificat. Il est important de spécifier l'adresse Internet finale qui sera utilisée pour accéder au WCS dans le domaine NC du DN afin d'éviter des avertissements de navigateur.Voici un exemple :**C:\Program Files\WCS4.1\bin>keyadmin -newdn -csr genkey C:\TEST\CSR-WCS.PEMThe WCS server is runningChanges will take affect on the next server restartEnter the domain name of the server: TS-WEBEnter the name of your organizational unit: ABCEnter the name of your organization: XYZEnter the name of your city or locality: SanjoseEnter the name of your state or province: CAEnter the two letter code for your country: USGenerating RSA keyConfiguring Apache server for keyWriting certificate signing request to C:\TEST\CSR-WCS.PEM**Une fois que la commande est exécutée, les informations CSR sont générées et écrites au fichier.Les informations CSR ressemblent à ceci :**C:\Program Files\WCS4.1\bin>keyadmin -newdn -csr genkey C:\TEST\CSR-WCS.PEMThe WCS server is runningChanges will take affect on the next server restartEnter the domain name of the server: TS-WEBEnter the name of your organizational unit: ABCEnter the name of your organization: XYZEnter the name of your city or locality: SanjoseEnter the name of your state or province: CAEnter the two letter code for your country: USGenerating RSA keyConfiguring Apache server for keyWriting certificate signing request to C:\TEST\CSR-WCS.PEM**Maintenant que votre CSR est prêt, copiez et collez les informations CSR dans n'importe quel outil d'inscription CA.Afin de copier et coller les informations dans la forme d'inscription, ouvrez le fichier dans un éditeur de texte qui n'ajoute pas les caractères supplémentaires. Cisco recommande que vous utilisiez Microsoft Notepad ou UNIX VI. Référez-vous au site Web de la tierce partie CA pour plus d'informations sur la façon soumettre le CSR par l'outil d'inscription.Après que vous soumettiez le CSR à la tierce partie CA, la tierce partie CA digitalement signe le certificat et envoie de retour le certificat signé par l'intermédiaire de l'email.Une fois que vous récupérez le certificat signé du CA, vous pouvez l'installer pour remplacer le certificat auto-signé par original en écrivant cette commande :**keyadmin importsignedcert** [certFileName]Le certificat et la clé sont enregistrés à **C:\ProgramFiles\WCS4.1\webnms\apache\conf\ssl.crt**.Le certificat devrait être une certification X.509 signée dans le format PEM, et il doit apparier la clé privée qui a été initialement générée par la commande de **genkey** (voir l'étape 1). Par conséquent, si vous générez une clé de nouveau avant que vous importiez le certificat, il rejettera le certificat.

Importez une clé/paire préexistantes de certificat au WCS

Le WCS a également des dispositions d'importer une clé/paire préexistantes de certificat. Afin d'exécuter ceci, sélectionnez cette commande :

keyadmin importkey *[keyFileName] [certFileName]*

La clé doit être une clé privée PEM-encodée RSA avec une ligne par laquelle commence COMMENCENT LA CLÉ PRIVÉE RSA, ou ce peut être une clé privée PEM-encodée RSA dans le format PKCS8 avec une ligne par laquelle commence COMMENCENT LA CLÉ PRIVÉE. Dans l'un ou l'autre de cas, la clé ne doit pas être protégée par mot de passe.

Le certificat devrait être un certificat X.509 PEM-encodé qui apparie la clé.

Importez un certificat de serveur avec l'intermédiaire CAs

Si le certificat de serveur SSL est signé par un intermédiaire CA, pour s'assurer que WCS passe de retour le plein trousseau de clés CA, vous devez combiner le certificat de serveur, l'intermédiaire CAs et le certificat de CA de racine dans un nouveau certificat PEM :

keyadmin importkey *[keyFileName] [certFileName]*
Ce nouveau fichier du certificat PEM est [certFileName] pour être utilisé avec les commandes :

keyadmin importkey *[keyFileName] [certFileName]*

Vérifiez

Terminez-vous ces étapes afin de vérifier si la configuration fonctionne comme prévu :

1. Après que vous importiez le certificat signé en fonction au WCS, redémarrez le WCS pour les modifications pour le prendre effet.
2. Accédez au WCS par le navigateur Web.Si le certificat signé est valide et a un nom de domaine assorti, l'utilisateur doit aller juste à la page de connexion sans problème avec le dialogue d'avertissement instantané de certificat.

Dépannez

L'outil Keyadmin.bat ne génèrera pas le CSR installent dedans le répertoire

Quand **keyadmin.bat** est exécuté dans le WCS **\ répertoire de coffre** sur Windows, cette erreur apparaît :

```
Generating RSA keyConfiguring Apache server for keyWriting certificate signing request toError
generating key java.security.KeyStoreException: Could not create CSRC:\Program Files\WCS4.x\bin>
```

Afin de résoudre ce problème, définissez un nom du fichier dans un autre répertoire sans compter que le répertoire d'installation du WCS. Voici un exemple :

```
C:\Program Files\WCS4.2.81.0\bin>keyadmin -newdn -csr genkey C:\TEST\CSR-WCS.PEMThe WCS server
is runningChanges will take affect on the next server restartEnter the domain name of the
server: ciscoEnter the name of your organizational unit: ciscoEnter the name of your
organization: ciscoEnter the name of your city or locality: SJEnter the name of your state or
province: CAEnter the two letter code for your country: USGenerating RSA keyConfiguring Apache
server for key\Writing certificate signing request to C:\TEST\CSR-WCS.PEM
```

Informations connexes

- Génération de la demande de signature de certificat (CSR) pour un tiers certificat sur un contrôleur WLAN (WLC)
- Dépannage du système de contrôle sans fil
- Page de prise en charge du mode sans fil
- Support et documentation techniques - Cisco Systems