Soutien principal de bit aie 2048 de CSR sur l'exemple de configuration aie

Contenu

Introduction

Ce document décrit comment générer le soutien principal de 2048 bits de la demande de signature de certificat (CSR) sur l'appliance de Chiffrement Cisco IronPort (aie).

Configurez

La plupart des autorités de certification (CAs) ont énoncé une demande explicite pour avoir tout le CSRs généré avec une paire de clés de bit de la longueur 2048. Par défaut, la version 6.5 aie utilise la longueur principale de 1024 bits pour la génération de paire de clés. Afin de forcer l'aie pour générer une paire de clés de la longueur 2048, utilisez la commande de keytool comme décrit ici.

Générez un certificat

1. Procédure de connexion à l'aie CLI

2. Au menu principal, type **X** afin de relâcher dans le shell.

3. Modification à l'utilisateur de base :
```
$ su -
```

4. Exécutez le keytool afin de créer un nouveau keystore :
```
    # /usr/local/postx/server/jre/bin/keytool -genkey -alias <server alias>
-keyalg RSA -keysize 2048 -keystore <name the new keystore>
       *alias should be what the server is known as externally when customers
log into the device
       *When prompted for password use a easily remembered password
       *Enter in all requested information when prompted for the certificate
request, make special note of the next question:
       --- What is your first and last name?
```

```
       [Unknown]: server1.example.com
               *For this question enter in the fully qualified domain name
of the system
       *The name of the newkeystore should be in the format <name>.keystore
where name should include the current date
           Example:  enterpriseks20130108.keystore
```

5. Exécutez le keytool afin de créer un fichier CSR :
   # /usr/local/postx/server/jre/bin/keytool -certreq -keyalg RSA -alias <server alias> -file <servername>.csr -keystore <name of the new keystore>

6. Fournissez le fichier CSR à l'autorité de certification afin de générer un certificat. Assurez que vous le soumettez comme demande de signature d'Apache Web Server Certficate.
7. Après que vous receviez le fichier de .cer du CA, poursuivez aux étapes suivantes.

Importez un certificat

Remarque: Le mot de passe utilisé quand vous générez le CSR **doit** apparier le mot de passe de keystore pour que ces procédures fonctionnent. Si le CSR était hors fonction-case créée, le mot de passe entré **doit** apparier le mot de passe de keystore pour que ces procédures fonctionnent.

Vous devez enchaîner le certificat correctement

1. Chaque certificat de CA doit être extrait à partir du fichier CER reçu du CA et alors fusionné ensemble dans un éditeur de texte.

   Remarque: C'est plus facile fait d'un ordinateur de Microsoft Windows. D'autres systèmes d'exploitation fonctionnent mais sont plus difficiles à extraire.
   Des Certificats doivent être enchaînés dans cette commande : 1.Domain 2. 3.Root intermédiaire

   Double-cliquer afin d'ouvrir le fichier du certificat (fichier .CER), et puis cliquez sur l'onglet de **chemin de certification** :

   Le début avec l'à mi-niveau du chemin de certification, cliquent sur l'onglet de **détails**, cliquent sur la **copie pour classer**, et puis la nomment **1.CER**.

   Base-64 choisi **a encodé X.509(.CER)**.

La répétition pour le niveau supérieur CA, et le nomment **2.CER**.

La répétition pour le certificat de serveur, et **le nomment 3.CER**.

Employez un éditeur de texte (**pas** Notepad, mais les travaux notepad++ bien) afin d'ouvrir chacun des trois fichiers **X.CER** et les combiner dans la commande (1 au dessus, et 3 au bas) :

Remarque: Il ne devrait y avoir aucune ligne vide entre les Certificats et aucune ligne vide au bas.

Sauvegardez comme **<servername>.CER**.

Téléchargez le fichier **<servername>.CER à l'**aie chez **/home/admin/ <servername.cer>** avec le FTP ou le SCP.

Copie **/home/admin/ <servername.cer> à /usr/local/postx/server/conf :**

2. Utilisez le GUI aie afin d'importer le certificat [des clés et des Certificats **|** SSL installé].

   Remarque: Keystore = **[installez le répertoire] /conf/enterprisenamestore.keystore ou le** nom en cours de votre fichier de keystore.

   Certificat = **/usr/local/postx/server/conf/NEWCERT.CER**.

   CERT de la confiance CA de contrôle.

   Certificat d'importation de clic

3. (Facultatif -- Si un nouveau keystore doit être créé). Du GUI aie, dites l'aie d'utiliser le nouveau keystore :

   Choisissez la configuration **|** Serveur Web et proxys **|** Serveur Web **|** Auditeurs de connexion **|** HTTPS

Saisissez le chemin au nouveau fichier de keystore :

Exemple : ${postx.home}/conf/2013_5_13.keystore

4. Déployez les modifications et redémarrez l'adaptateur de SMTP.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.