Générez un CSR avec le guide de nom secondaire dans le ravitaillement principal de Collaboration (PCP)

Contenu

Introduction

Ce document décrit comment générer une demande de signature de certificat (CSR) dans le ravitaillement principal de tenir compte des noms secondaires.

Conditions préalables

Conditions requises

- Un Autorité de certification (CA) devra signer le certificat que vous générez de PCP, vous pouvez utiliser des Windows Server ou avoir un signe CA il en ligne.

Si vous êtes incertain comment faire signer votre certificat par une ressource en ligne CA, s'il vous plaît mettez en référence le lien ci-dessous

https://www.digicert.com/

- La racine Access à l'interface de ligne de commande (CLI) du ravitaillement principal sera nécessaire. L'accès de racine est généré au moment installent.

> Remarque: Pour PCP les versions 12.X et satisfont en haut se rapportent au bas de ce document sous d'autres notes

Composants utilisés

Ravitaillement principal de Collaboration

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 vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Informations générales

Ceci te permettra pour accéder au ravitaillement principal de Collaboration (PCP) à des fins commerciales avec de plusieurs entrées de Domain Name Server (DN) utilisant le même certificat et pour ne pas rencontrer l'erreur de certificat quand vous accédez à la page Web.

Procédure et mesures

Au moment de ce wasw de document écrit, de l'interface utilisateur graphique (GUI) vous pouvez seulement générer le CSR sans le nom secondaire, ceux-ci êtes les instructions d'accomplir cette tâche.

Étape 1. Procédure de connexion à PCP en tant qu'utilisateur de base

Étape 2. Naviguez vers **/opt/cupm/httpd/** par le **cd /opt/cupm/httpd/ d'**entrée

Étape 3. Type : **vi san.cnf**

Remarque: Ceci créera un nouveau fichier appelé le san.cnf qui sera vide à l'heure actuelle

Étape 4. Appuyez sur **I** pour l'insertion (ceci laissera éditer le fichier) et la copie/pâte le ci-dessous dans le domaine gris

Veuillez noter aussi bien l'entrée au bas DNS.1 = pcptest23.cisco.ab.edu est l'entrée de DNS principal qui sera utilisée pour le CSR et le DNS.2 sera la secondaire ; De cette façon vous pouvez accéder à PCP et utiliser l'un ou l'autre des entrées DNS.

Après qu'une copie/pâte dans cet exemple, retirent s'il vous plaît les exemples pcptest avec ceux vous avez besoin pour votre application.

```
[ req ] default_bits = 2048 distinguished_name = req_distinguished_name req_extensions = req_ext [
req_distinguished_name ] countryName = Country Name (2 letter code) stateOrProvinceName = State or Province Name
(full name) localityName = Locality Name (eg, city) organizationName = Organization Name (eg, company) commonName =
Common Name (e.g. server FQDN or YOUR name) [ req_ext ] subjectAltName = @alt_names [alt_names] DNS.1 =
pcptest23.cisco.ab.edu DNS.2 = pcptest.gov.cisco.ca
```

Étape 5. Type : **ESC** tapent alors **: wq !** (ceci sauvegardera le fichier et les modifications juste apportés).

Étape 6. Services de reprise pour que le fichier de config prenne l'affect correctement. Type : **arrêt de /opt/cupm/bin/cpcmcontrol.sh**

l'état de /opt/cupm/bin/cpcmcontrol.sh de type pour assurer tous les services ont arrêté

Étape 7. Introduisez cette commande de permettre aux services pour se réactiver : **début de /opt/cupm/bin/cpcmcontrol.sh**

Étape 8. Vous devriez encore être dans le répertoire de **/opt/cupm/httpd/**, vous pouvez taper le **pwd** pour trouver votre répertoire courant pour s'assurer.

Étape 9. Exécutez cette commande de générer la clé privée et le CSR.

req d'openssl - PCPSAN.csr - newkey rsa:2048 - Noeuds - keyout private.key - config san.cnf

```
[root@ryPCP11-5 httpd]# openssl req -out PCPSAN.csr -newkey rsa:2048 -nodes -keyout private.key -config san.cnf
Generating a 2048 bit RSA private key .........+++ .........+++ writing new private key to 'private.key' ----- You
are about to be asked to enter information that will be incorporated into your certificate request. What you are
about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some
blank For some fields there will be a default value, If you enter '.', the field will be left blank. ----- Country
Name (2 letter code) []:US State or Province Name (full name) []:TX Locality Name (eg, city) []:RCDN Organization
Name (eg, company) []:CISCO Common Name (e.g. server FQDN or YOUR name) []:doctest.cisco.com [root@ryPCP11-5 httpd]#
```

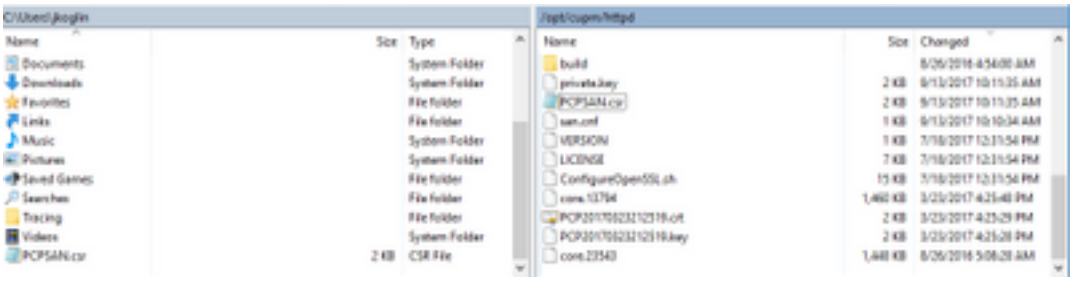
Le CSR obtient généré et pour vérifier si le CSR contient le type correct de noms secondaires cette commande

req d'openssl - noout - texte - dans PCPSAN.csr | DN de grep

```
[root@ryPCP11-5 httpd]# openssl req -noout -text -in PCPSAN.csr | grep DNS DNS:pcptest23.cisco.ab.edu,
DNS:pcptest.gov.cisco.ca [root@ryPCP11-5 httpd]#
```

> Remarque: Si les entrées DNS sont identiques que ci-dessous affichée l'étape 4, vous devriez voir les mêmes que vous êtes entré dans l'étape 4. Après que vous le vérifiiez, poursuivez à l'étape suivante

Étape 10. Utilisez un programme appelé le winscp ou le filezilla se connectent à PCP en tant qu'utilisateur de base et naviguent vers le répertoire de **/opt/cupm/httpd/** et déplacent le .csr du serveur PCP à votre appareil de bureau.



Étape 11. Signez le CSR avec votre CA et utilisez les fenêtres serveur ou en ligne par l'intermédiaire d'un constructeur tiers tel que DigiCert.

Étape 12. Installez le certificat PCP dans le GUI, naviguez : **Certificats d'Administration>Updates>SSL.**

Étape 13. Installez le certificat par votre navigateur, des références par navigateur est en tant que ci-dessous.

Google Chrome :

https://www.tbs-certificates.co.uk/FAQ/en/installer_certificat_client_google_chrome.html

Internet Explorer :

http://howtonetworking.com/Internet/iis8.htm

https://support.securly.com/hc/en-us/articles/206082128-Securly-SSL-certificate-manual-install-in-Internet-Explorer

Mozilla Firefox :

https://wiki.wmtransfer.com/projects/webmoney/wiki/Installing_root_certificate_in_Mozilla_Firefox

Étape 14. Après que vous installiez le certificat sur le serveur et votre navigateur, effacez le cache et fermez-vous hors du navigateur.

Étape 15. Rouvrez l'URL et vous ne devriez pas rencontrer l'erreur de sécurité.

D'autres notes

> Remarque: Version 12.x et ultérieures PCP vous avez besoin de TAC pour te fournir l'accès CLI pendant que ceci est limité.

Processus pour demander CLI Access

Étape 1. Procédure de connexion au GUI PCP

Étape 2. Naviguez vers **Administration>Logging et Showtech>Click sur l'account>create de dépannage l'ID utilisateur** et sélectionnez un temps approprié que vous avez besoin de l'accès de racine pour accomplir ceci.

Étape 3. Fournissez au TAC la chaîne de défi et ils te fourniront le mot de passe (ce mot de passe sera très prolongé, ne l'inquiète pas fonctionnera).

```
Example:
AQAAAAEAAAC8srFZB2prb2dsaW4NSm9zZXBoIEtvZ2xpbgAAAbgBAAIBAQIABAAA FFFFEBE0
AawDAJEEAEBDTj1DaXNjb1N5c3RlbXM7T1U9UHJpbWVDb2xsYWJvcmF0aW9uUHJv FFFFEB81
dmlzaW9uaW5nO089Q2lzY29TeXN0ZW1zBQAIAAAAAFmxsrwGAEBDTj1DaXNjb1N5 FFFFEB8A
c3RlbXM7T1U9UHJpbWVDb2xsYWJvcmF0aW9uUHJvdmlzaW9uaW5nO089Q2lzY29T FFFFEAD0
eXN0ZW1zBwABAAgAAQEJAAEACgABAQsBAJUhvhhxkM6YNYVFRPT3jcqAsrl/1ppr FFFFEB2B
yr1AYzJa9FtO1A4l8VBlp8IVqbqHrrCAIYUmVXWnzXTuxtWcY2wPSsIzW2GSdFZM FFFFE9F3
LplEKeEX+q7ZADshWeSMYJQkY7I9oJTfD5P4QE2eHZ2opiiCScgf3Fii6ORuvhiM FFFFEAD9
kbbO6JUguABWZU2HV0OhXHfjMZNqpUvhCWCCIHNKfddwB6crb0yV4xoXnNe5/2+X FFFFEACE
7Nzf2xWFaIwJOs4kGp5S29u8wNMAIb1t9jn7+iPg8Rezizeu+HeUgs2T8a/LTmou FFFFEA8F
Vu9Ux3PBOM4xIkFpKa7provli1PmIeRJodmObfS1Y9jgqb3AYGgJxMAMAAFB6w== FFFFEAA7
DONE.
```

Étape 4. Déconnexion de votre utilisateur courant et procédure de connexion avec l'ID utilisateur que vous avez créé et le mot de passe fourni par TAC.

Étape 5. Naviguez vers **dépanner Account>>Launch>>Click sur le compte de console** et créez votre user-id et mot de passe cli.

Étape 6. Maintenant ouvrez une session à PCP comme l'utilisateur que vous avez créé et exécutez les mesures initiales décrites dans ce document.