Een CSR met alternatieve naamgids genereren in Prime Collaboration Provisioning (PCP)

Inhoud

Inleiding

Dit document beschrijft hoe u een certificaataanvraag (CSR) kunt genereren in de primaire voorziening om alternatieve namen toe te staan.

Voorwaarden

Vereisten

- Een certificaatinstantie (CA) moet het certificaat ondertekenen dat u met PCP gegenereerd hebt, u kunt een Windows-server gebruiken of u kunt een CA-teken gebruiken online.

Als u niet zeker weet hoe uw Certificaat door een CA online bron ondertekend is, verwees dan naar de onderstaande link

https://www.digicert.com/

- Er is Root Access to the Opdracht Line Interface (CLI) van de Prime Provisioning vereist. Root access wordt gegenereerd op Installeer.

> Opmerking: Raadpleeg voor PCP-versie(s) 12.X en hoger de onderkant van dit document onder Aanvullende opmerkingen

Gebruikte componenten

Prime-provisioning voor samenwerking

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Hierdoor kunt u met hetzelfde certificaat toegang krijgen tot de Prime Collaboration Provisioning (PCP) voor bedrijfsdoeleinden met meerdere DNS-items van Domain Name Server (DNS) en krijgt u niet de certificaatfout bij toegang tot de webpagina.

Procedure en stappen

Op het moment dat dit document is geschreven, kunt u vanuit de GUI (Graphical User Interface - grafische gebruikersinterface) alleen de CSR zonder alternatieve naam genereren, dit zijn de instructies om deze taak te volbrengen.

Stap 1. Meld u aan bij PCP als basisgebruiker

Stap 2. Navigeren naar **/opt/cupm/httpd/**door de input **cd**/opt/cupm/httpd/

Stap 3. Type: **vi san.cnf**

> Opmerking: Dit maakt een nieuw bestand, san.cnf genaamd, dat op het moment leeg zal zijn

Stap 4. Druk op **I** voor invoeging (dit maakt het mogelijk het bestand te bewerken) en kopieer/plak de onderstaande tekst in het grijze veld

Merk ook op dat de vermelding op de onderste DNS.1 = pcptest23.cisco.ab.edu de primaire DNS-ingang is die gebruikt zal worden voor de CSR en DNS.2 de secundaire DNS-ingang is; Op deze manier hebt u toegang tot PCP en kunt u een van de DNS-items gebruiken.

Nadat u een kopie/pasta in dit voorbeeld hebt gemaakt, verwijdert u de voorbeeldvoorbeelden met de voorbeelden die u voor uw toepassing nodig hebt.

```
[ 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
```

Stap 5. Type: **esc** type **: wq !** (hierdoor worden het bestand en de zojuist aangebrachte wijzigingen opgeslagen).

Stap 6. Herstart van de diensten voor de configuratie van het bestand op de juiste wijze. Type: **/opt/cupm/bin/cpcmcontrol.sh stop**

type **/opt/cupm/bin/cpcmcontrol.sh status** om er zeker van te zijn dat alle services zijn gestopt

Stap 7. Typ deze opdracht om de services weer te geven: **/opt/cupm/bin/cpcmcontrol.sh**

Stap 8. U dient nog steeds in de **folder/opt/cupm/httpd/**folder te zijn, u kunt **pwd** typen om uw huidige directory zeker te stellen.

Stap 9. Start deze opdracht om de Private key en CSR te genereren.

openssl req-out PCPSAN.csr-newkey rsa:2048-knooppunten -keyout PCPSAN.key-grotere 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]#
```

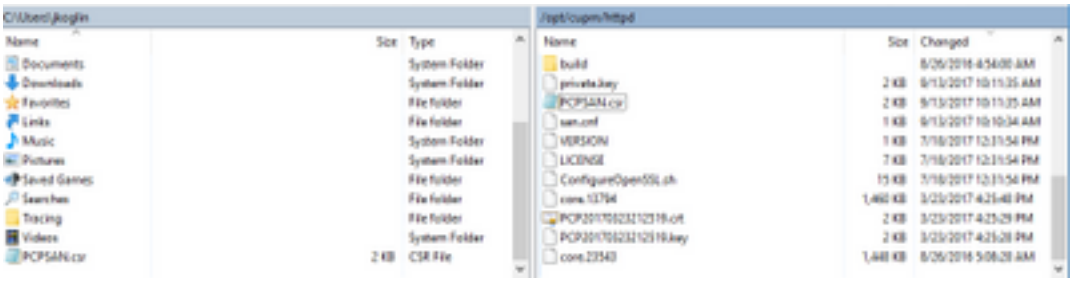
CSR wordt gegenereerd en om te controleren of CSR de juiste alternatieve namen bevat type deze opdracht

openssl req -noout-tekst in PCPSAN.csr | DNS-griep

```
[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]#
```

> Opmerking: Als de DNS-items dezelfde zijn als die onder stap 4 staan, dient u hetzelfde te zien als u in stap 4 hebt ingevoerd. Nadat u dit hebt geverifieerd, gaat u naar de volgende stap

Stap 10. Gebruik een programma dat winscp of fiLezilla heet, sluit aan op PCP als wortelgebruiker en navigeer naar de **/opt/cupm/httpd/**folder en verplaats de .csr van de PC server naar uw desktop.



Stap 1. Teken de CSR met uw CA en gebruik een Windows-server of online via een derde verkoper zoals DigiCert.

Stap 12. Installeer het PCP-certificaat in de GUI, navigeer: **Administratie>updates>SSL-certificaten.**

Stap 13. Installeer het certificaat via uw browser, de referenties per browser zijn zoals hieronder.

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

Stap 14. Nadat u het certificaat op de server en uw browser installeert, ontkoppel het cache en sluit het browser af.

Stap 15. Open de URL opnieuw en u dient de beveiligingsfout niet te ervaren.

Opmerkingen

> Opmerking: PCP versie 12.x en hoger heeft u TAC nodig om u de CLI Access te bieden aangezien dit beperkt is.

Procedure om CLI-toegang aan te vragen

Stap 1. Meld u aan bij PCP-GUI

Stap 2. Navigeer naar **Administratie>Vastlegging en technologie>Klik op account voor probleemoplossing>maak de gebruiker** en selecteer een geschikte tijd die u basistoegang nodig hebt om dit te bereiken.

Stap 3. Geef aan TAC de challenge string en zij zullen u het wachtwoord geven (dit wachtwoord is

zeer lang en maakt u geen zorgen dat het werkt).

```
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.
```

Stap 4. Meld de huidige gebruiker aan en logt u in met de door u aangemaakte gebruiker en het wachtwoord dat door TAC wordt geleverd.

Stap 5. **Navigeer** naar **account voor probleemoplossing>>Start>>Klik op een console-account** en maak uw CLI-gebruikersid en -wachtwoord aan.

Stap 6. Meld u nu aan bij PCP als de gebruiker die u hebt gemaakt en voer de eerste stappen uit die in dit document zijn beschreven.

> Opmerking: PCP versie 12.x en hoger moet u eerst in de opdrachtregel invoeren voordat u alle instructies voor het uitvoeren uitvoert. Voor stap 9 zal de opdracht daarom **sudo openssl req-out PCPSAN.csr-newkey rsa:2048-knooppunten -keyout PCPSAN.key-grotere san.cnf zijn.** Om de DNS te controleren gebruikt u vervolgens de opdrachtregel **doop enssl req -no-text -in PCPSAN.csr | DNS-griep**