Erstellen eines CSR mit Alternate Name Guide in Prime Collaboration Provisioning (PCP)

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie eine CSR-Anfrage (Certificate Signing Request) in der primären Bereitstellung generiert wird, um alternative Namen zuzulassen.

Voraussetzungen

Anforderungen

- Eine Zertifizierungsstelle (Certificate Authority, CA) muss das Zertifikat signieren, das Sie von PCP generieren. Sie können einen Windows-Server verwenden oder es online mit einer Zertifizierungsstelle signieren lassen.

Wenn Sie nicht sicher sind, wie Ihr Zertifikat von einer CA-Online-Ressource signiert wird, verweisen Sie bitte auf den unten stehenden Link.

https://www.digicert.com/

- Der Root-Zugriff auf die Befehlszeilenschnittstelle (CLI) des Prime Provisioning wird benötigt. Der Root-Zugriff wird bei der Installation generiert.

> **Hinweis**: Weitere Hinweise zu PCP-Versionen 12.X und höher finden Sie am Ende dieses Dokuments.

Verwendete Komponenten

Prime Collaboration-Bereitstellung

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie

die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Auf diese Weise können Sie für geschäftliche Zwecke mit mehreren DNS-Einträgen (Domain Name Server), die dasselbe Zertifikat verwenden, auf das Prime Collaboration Provisioning (PCP) zugreifen, ohne dass beim Zugriff auf die Webseite ein Zertifikatfehler auftritt.

Verfahren und Schritte

Zum Zeitpunkt der Erstellung dieses Dokuments können Sie über die grafische Benutzeroberfläche (GUI) nur den CSR ohne alternativen Namen generieren. Dies sind die Anweisungen zum Ausführen dieser Aufgabe.

Schritt 1: Melden Sie sich bei PCP als Root-Benutzer an.

Schritt 2: Navigieren Sie zu **/opt/cupm/httpd/**über die Eingabe **cd**/opt/cupm/httpd/.

Schritt 3: Typ: **vi san.cnf**

Hinweis: Dadurch wird eine neue Datei namens san.cnf erstellt, die im Moment leer ist.

Schritt 4: Drücken Sie **I**, um die Datei einzufügen (dadurch können Sie sie bearbeiten), und kopieren Sie den Text unten in das graue Feld.

Beachten Sie auch den Eintrag unten DNS.1 = pcptest23.cisco.ab.edu ist der primäre DNS-Eintrag, der für den CSR verwendet wird, und der Eintrag DNS.2 ist der sekundäre Eintrag. Auf diese Weise können Sie auf PCP zugreifen und einen der DNS-Einträge verwenden.

Entfernen Sie nach dem Kopieren bzw. Einfügen in dieses Beispiel die Beispielpackungen mit den Beispielen, die Sie für Ihre Anwendung benötigen.

```
[ 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
```

Schritt 5: Typ: **esc** geben Sie dann **:wq!** (dies speichert die Datei und die vorgenommenen Änderungen).

Schritt 6: Starten Sie die Dienste neu, damit die Konfigurationsdatei ordnungsgemäß funktioniert. Geben Sie Folgendes ein: **/opt/cupm/bin/cpcmcontrol.sh stop**

Geben Sie **/opt/cupm/bin/cpcmcontrol.sh ein**, um sicherzustellen, dass alle Dienste beendet wurden.

Schritt 7: Geben Sie diesen Befehl ein, damit die Dienste wieder verfügbar sind: **/opt/cupm/bin/cpcmcontrol.sh**

Schritt 8: Sie sollten sich immer noch im **/opt/cupm/httpd/**directory befinden, können Sie **pwd** eingeben, um Ihr aktuelles Verzeichnis zu finden.

Schritt 9: Führen Sie diesen Befehl aus, um den privaten Schlüssel und CSR zu generieren.

openssl req -out PCPSAN.csr -newkey rsa:2048 -knoten -keyout PCPSAN.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]#
```

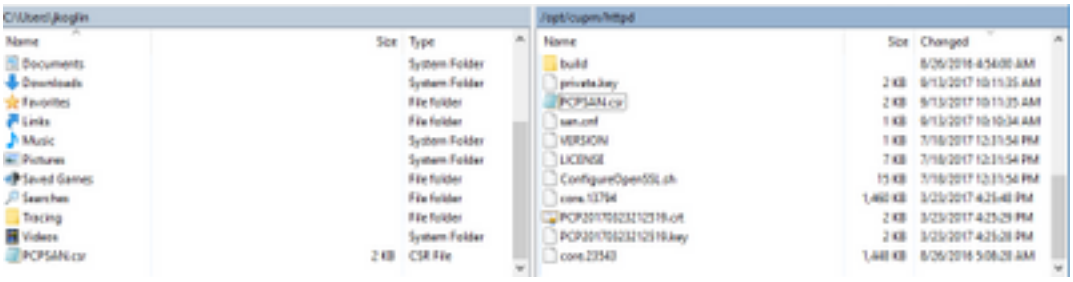
Der CSR wird generiert, und um zu überprüfen, ob der CSR die richtigen alternativen Namen enthält, geben Sie diesen Befehl ein.

openssl req -noout -text in PCPSAN.csr | grep DNS

```
[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]#
```

> **Hinweis**: Wenn die DNS-Einträge die gleichen sind wie in Schritt 4 dargestellt, sollten Sie die gleichen sehen, die Sie in Schritt 4 eingegeben haben. Fahren Sie nach der Überprüfung mit dem nächsten Schritt fort.

Schritt 10: Verwenden Sie ein Programm mit dem Namen winscp oder filezilla connect als root, und navigieren Sie zum **Verzeichnis /opt/cupm/httpd/**und verschieben Sie die CSR-Datei vom PCP-Server auf Ihren Desktop.



Schritt 11: Signieren Sie den CSR mit Ihrer CA, und verwenden Sie entweder einen Windows-Server oder online über einen Drittanbieter wie DigiCert.

Schritt 12: Installieren Sie das PCP-Zertifikat in der GUI. Navigieren Sie zu: **Administration>Updates>SSL-Zertifikate.**

Schritt 13: Installieren Sie das Zertifikat über Ihren Browser, Referenzen pro Browser ist wie unten.

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

Schritt 14: Nachdem Sie das Zertifikat auf dem Server und in Ihrem Browser installiert haben, löschen Sie den Cache, und schließen Sie den Browser.

Schritt 15: Öffnen Sie die URL erneut, und es sollte kein Sicherheitsfehler auftreten.

Weitere Hinweise

> Hinweis: Für PCP ab Version 12.x ist TAC erforderlich, um Ihnen den CLI-Zugriff zu ermöglichen, da dies eingeschränkt ist.

Prozess zum Anfordern des CLI-Zugriffs

Schritt 1: Anmeldung bei der PCP-GUI

Schritt 2: Navigieren Sie zu **Administration > Logging and Showtech > klicken Sie auf Troubleshooting account > Create the userID (Benutzererkennung erstellen),** und wählen Sie die

entsprechende Zeit aus, zu der Sie Root-Zugriff benötigen, um dies zu erreichen.

Schritt 3: Geben Sie dem TAC die Challenge und sie geben Ihnen das Passwort (dieses Passwort ist sehr lang, keine Sorge, es wird funktionieren).

```
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.
```

Schritt 4: Melden Sie sich mit der von Ihnen erstellten Benutzer-ID und dem vom TAC bereitgestellten Kennwort ab.

Schritt 5: Navigieren Sie zu **Troubleshooting Account>>Launch>>Klicken Sie auf Console Account** und erstellen Sie Ihre CLI-Benutzer-ID und Ihr Kennwort.

Schritt 6: Melden Sie sich jetzt als Benutzer bei PCP an, den Sie erstellt haben, und führen Sie die in diesem Dokument beschriebenen ersten Schritte aus.

> Hinweis: PCP ab Version 12.x müssen Sie den Befehl **sudo** eingeben, bevor alle Anweisungen für die Funktion ausgeführt werden. Für Schritt 9 lautet der Befehl daher **sudo openssl req -out PCPSAN.csr -newkey rsa:2048 -knoten -keyout PCPSAN.key -config san.cnf.** Um die DNS zu überprüfen, verwenden Sie den Befehl **sudoopenssl req -noout -text -in PCPSAN.csr. | grep DNS**