Generare un CSR con la guida dei nomi alternativi in Prime Collaboration Provisioning (PCP)

Sommario

Introduzione

In questo documento viene descritto come generare una richiesta di firma del certificato (CSR) nel provisioning principale per consentire nomi alternativi.

Prerequisiti

Requisiti

- Un'Autorità di certificazione (CA) dovrà firmare il certificato generato da PCP, è possibile utilizzare un server Windows o farlo firmare online da un CA.

Se non si è certi della modalità di firma del certificato da parte di una risorsa online della CA, fare riferimento al collegamento seguente

https://www.digicert.com/

- Sarà necessario l'accesso root all'interfaccia della riga di comando (CLI) di Prime Provisioning. L'accesso alla radice viene generato al momento dell'installazione.

> **Nota:** Per le versioni PCP 12.X e successive, fare riferimento alla parte inferiore di questo documento in Ulteriori note

Componenti usati

Prime Collaboration Provisioning

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo modo sarà possibile accedere a Prime Collaboration Provisioning (PCP) per scopi aziendali con più voci DNS (Domain Name Server) utilizzando lo stesso certificato e non si verificherà l'errore del certificato quando si accede alla pagina Web.

Procedura e passaggi

Al momento della stesura del presente documento, dall'interfaccia utente grafica (GUI) è possibile generare il CSR solo senza un nome alternativo. Di seguito sono riportate le istruzioni per eseguire questa operazione.

Passaggio 1. Accedere a PCP come utente root

Passaggio 2. Passare a **/opt/cupm/httpd/** tramite il **cd di** input **/opt/cupm/httpd/**

Passaggio 3. Digitare: **vi san.cnf**

> **Nota:** Verrà creato un nuovo file denominato san.cnf che sarà vuoto al momento

Passaggio 4. Premere **I** per inserire (in modo da poter modificare il file) e copiare/incollare quanto segue nel campo grigio

Si noti inoltre che la voce in basso DNS.1 = pcptest23.cisco.ab.edu è la voce DNS primaria che verrà utilizzata per CSR e DNS.2 sarà la voce secondaria; In questo modo è possibile accedere a PCP e utilizzare una delle voci DNS.

Dopo aver copiato/incollato l'esempio, rimuovere gli esempi pcptest con quelli necessari per l'applicazione.

```
[ 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
```

Passaggio 5. Digitare: **esc,** quindi digitare **:wq!** (il file e le modifiche appena apportate verranno salvati).

Passaggio 6. Per rendere effettivo il file di configurazione, riavviare i servizi. Digitare: **/opt/cupm/bin/cpcmcontrol.sh stop**

digitare **/opt/cupm/bin/cpcmcontrol.sh status** per verificare che tutti i servizi siano stati arrestati

Passaggio 7. Digitare questo comando per consentire il ripristino dei servizi: **/opt/cupm/bin/cpcmcontrol.sh start**

Passaggio 8. È comunque necessario trovarsi nella directory **/opt/cupm/httpd/**, è possibile digitare **pwd** per trovare la directory corrente per essere certi.

Passaggio 9. Eseguire questo comando per generare la chiave privata e CSR.

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

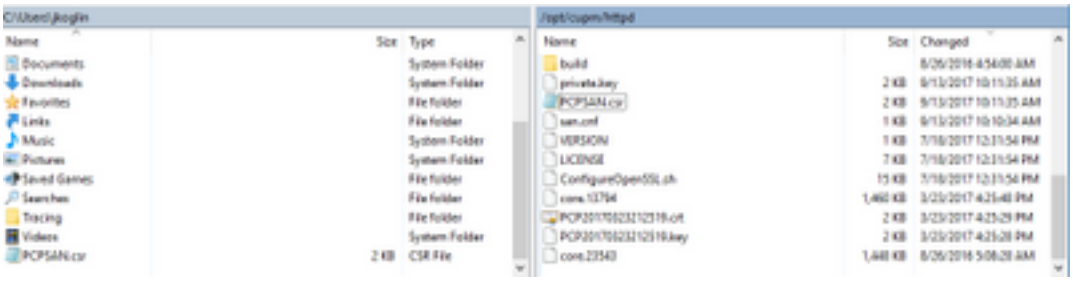
Il CSR viene generato e per verificare se contiene i nomi alternativi corretti digitare questo comando

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]#
```

> **Nota:** Se le voci DNS corrispondono a quelle mostrate al passaggio 4, dovrebbe essere visualizzato lo stesso valore immesso al passaggio 4. Dopo averlo verificato, procedere al passaggio successivo

Passaggio 10. Utilizzare un programma denominato winscp o filezilla connettersi a PCP come utente root e passare alla directory **/opt/cupm/httpd/** e spostare il file .csr dal server PCP al desktop.



Passaggio 11. Firmare il CSR con la CA e utilizzare un server Windows o in linea tramite un fornitore di terze parti, ad esempio DigiCert.

Passaggio 12. Installare il certificato PCP nella GUI, Navigare: **Amministrazione>Aggiornamenti>Certificati SSL.**

Passaggio 13. Installare il certificato tramite il browser. I riferimenti per browser sono i seguenti.

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

Passaggio 14. Dopo aver installato il certificato sul server e sul browser, cancellare la cache e chiudere il browser.

Passaggio 15. Riaprire l'URL e l'errore di sicurezza non dovrebbe verificarsi.

Ulteriori note

Nota: PCP versione 12.x e successive è necessario disporre di TAC per poter accedere alla CLI, in quanto è soggetto a restrizioni.

Processo di richiesta dell'accesso CLI

Passaggio 1. Accedere all'interfaccia utente di PCP

Passaggio 2. Passare a **Amministrazione>Log and Showtech>Fare clic sull'account per la risoluzione dei problemi>creare l'ID utente** e selezionare il momento appropriato in cui sarà

necessario l'accesso alla directory principale.

Passaggio 3. Fornire a TAC la stringa di richiesta e la password (questa password sarà molto lunga, non preoccuparsi che funzionerà).

```
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.
```

Passaggio 4. Uscire dall'utente corrente e accedere con l'ID utente creato e la password fornita da TAC.

Passaggio 5. Passare a **Risoluzione dei problemi - Account>>Avvio>>Fare clic sull'account console** e creare l'ID utente e la password della CLI.

Passaggio 6. Accedere a PCP come utente creato ed eseguire i passaggi iniziali descritti in questo documento.

> Nota: PCP versione 12.x e successive è necessario immettere il comando **sudo** prima di tutte le istruzioni per il corretto funzionamento. Per il passo 9, il comando sarà **sudo openssl req -out PCPSAN.csr -newkey rsa:2048 -nodes -keyout PCPSAN.key -config san.cnf.** Per verificare il DNS, utilizzare il comando **sudoopenssl req -noout -text -in PCPSAN.csr | GREP DNS**