Genere un CSR con la guía del nombre alterno en el aprovisionamiento primero de la Colaboración (PCP)

Contenido

Introducción

Este documento describe cómo generar un pedido de firma de certificado (CSR) en el aprovisionamiento primero de tener en cuenta los nombres alternos.

Prerequisites

Requisitos

- Un Certificate Authority (CA) necesitará firmar el certificado que usted genera de PCP, usted puede utilizar a un Servidor Windows o tener una muestra de CA él en línea.

Si usted es inseguro cómo hacer su certificado firmar por un recurso en línea de CA, por favor refiérase al link abajo

https://www.digicert.com/

- El acceso a raíz al comando line interface(cli) del aprovisionamiento primero será necesario. El acceso a raíz se genera sobre instala.

> **Note**: Para PCP las versiones 12.X y arriba satisfacen refieren a la parte inferior de este documento bajo otras notas

Componentes Utilizados

Aprovisionamiento primero de la Colaboración

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Antecedentes

Esto permitirá que usted acceda el aprovisionamiento primero de la Colaboración (PCP) con fines comerciales con las entradas múltiples del Domain Name Server (DNS) usando el mismo certificado y que no encuentre el error del certificado cuando usted accede la página web.

Procedimiento y pasos

A la hora de este wasw del documento escrito, del Interfaz gráfica del usuario (GUI) usted puede generar solamente el CSR sin el nombre alterno, éstos es las instrucciones de lograr esta tarea.

Paso 1. Login a PCP como el usuario raíz

Paso 2. Navegue a **/opt/cupm/httpd/** por el **Cd /opt/cupm/httpd/ de la** entrada

Paso 3. Tipo: **Vl san.cnf**

> **Note**: Esto creará un nuevo archivo llamado san.cnf que esté vacío en el momento

Paso 4. Presione **I** para el separador de millares (esto permitirá editar el archivo) y la copia/la goma el abajo en el campo gris

Observe por favor también la entrada en la parte inferior DNS.1 = pcptest23.cisco.ab.edu es la entrada de los DN primarios que será utilizada para el CSR y el DNS.2 será la secundaria; Esta manera usted puede acceder PCP y utilizar cualquiera de las entradas DNS.

Después de una copia/de una goma en este ejemplo, quite por favor los ejemplos más pcptest con los que usted necesita para su aplicación.

```
[ 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
```

Paso 5. Tipo: **salida** entonces teclea**: ¡wq!** (esto salvará el archivo y los cambios apenas realizados).

Paso 6. Servicios del reinicio para que el archivo de configuración tome la influencia correctamente. Tipo: **parada de /opt/cupm/bin/cpcmcontrol.sh**

el estatus de /opt/cupm/bin/cpcmcontrol.sh del tipo para asegurar todos los servicios ha parado

Paso 7. Teclee este comando de permitir que los servicios vengan salvaguardia: **comienzo de /opt/cupm/bin/cpcmcontrol.sh**

Paso 8. Usted debe todavía estar en el directorio de **/opt/cupm/httpd/**, usted puede teclear al **pwd** para encontrar su directorio actual para aseegurarse.

Paso 9. Funcione con este comando de generar la clave privada y el CSR.

req del openssl - hacia fuera PCPSAN.csr - newkey rsa:2048 - Nodos - 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]#
```

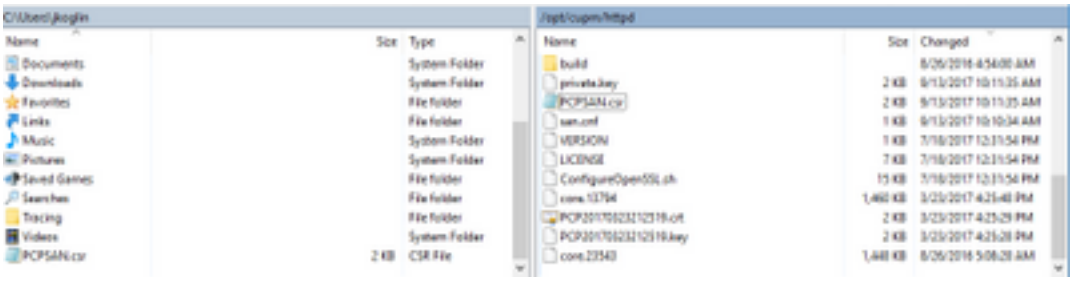
El CSR consigue generado y verificar si el CSR contiene el tipo correcto de los nombres alternos este comando

req del openssl - noout - texto - en 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]#
```

> **Note**: Si las entradas DNS son el mismo como se muestra abajo paso 4, usted debe ver lo mismo que usted ingresó en el paso 4. Después de que usted lo verifique, proceda al siguiente paso

Paso 10. Utilice un programa llamado winscp o el filezilla conecta con PCP como el usuario raíz y navega al directorio de **/opt/cupm/httpd/** y mueve el .csr desde el servidor PCP a su escritorio.



Paso 11 Firme el CSR con su CA y o utilice a un Servidor Windows o en línea vía los terceros proveedores tales como DigiCert.

Paso 12. Instale el certificado PCP en el GUI, navegue: **Certificados de Administration>Updates>SSL.**

Paso 13. Instale el certificado a través de su navegador, las referencias por el navegador está como abajo.

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

Paso 14. Después de que usted instale el certificado en el servidor y su navegador, borre el caché y al navegador cercano de los.

Paso 15. Abra de nuevo el URL y usted no debe encontrar el error de seguridad.

Otras notas

> Nota: Versión 12.x y posterior PCP usted necesita TAC proveer de usted el acceso CLI mientras que éste es restricto.

Proceso para pedir el acceso CLI

Paso 1. Login a PCP GUI

Paso 2. Navegue a **Administration>Logging y a Showtech>Click en el account>create del**

troubleshooting el userid y seleccione un momento apropiado que usted necesitará el acceso a raíz lograr esto.

Paso 3. Proporcione a TAC la cadena del desafío y le proporcionarán la contraseña (esta contraseña será muy muy larga, no se preocupa la trabajará).

```
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.
```

Paso 4. Logout de su Usuario usuario actual y login con el userid que usted creó y la contraseña proporcionada por TAC.

Paso 5. Navegue a **resolver problemas Account>>Launch>>Click en la cuenta de la consola** y cree su identificación del usuario y la contraseña cli.

Paso 6. Ahora inicie sesión a PCP como el usuario que usted creó y realice los pasos iniciales descritos en este documento.

> Nota: Versión 12.x y posterior PCP que usted necesita entrar en el **sudo del** comando antes de todas las instrucciones para que trabaje. Para el paso 9, el comando por lo tanto será **req del openssl del sudo - hacia fuera PCPSAN.csr - el newkey rsa:2048 - los Nodos - el keyout PCPSAN.key - los config san.cnf. Para verificar el** dns usted entonces utilizaría el sudoopensslreq del comando **- noout - texto - en PCPSAN.csr | grep DNS**