Gerencia um CSR com guia do nome alternativo no abastecimento principal da Colaboração (PCP)

Índice

Introdução

Este documento descreve como gerar uma solicitação de assinatura de certificado (CSR) no abastecimento principal permitir nomes alternativos.

Pré-requisitos

Requisitos

- Um Certificate Authority (CA) precisará de assinar o certificado que você gerencie de PCP, você pode usar um Windows Server ou ter um sinal de CA ele em linha.

Se você é incerto como ter seu certificado assinado por um recurso em linha de CA, por favor proveja o link abaixo

https://www.digicert.com/

- O acesso raiz ao comando line interface(cli) do abastecimento principal será precisado. O acesso raiz é gerado em cima instala.

> **Note**: Para PCP as versões 12.X e satisfazem acima referem a parte inferior deste documento sob umas notas mais adicionais

Componentes Utilizados

Abastecimento principal da Colaboração

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Informações de Apoio

Isto permitirá que você alcance o abastecimento principal da Colaboração (PCP) para fins comerciais com entradas múltiplas do Domain Name Server (DNS) usando o mesmo certificado e não encontre o erro do certificado quando você alcança o Web page.

Procedimento e etapas

Na altura deste wasw do documento escrito, da interface gráfica de usuário (GUI) você pode somente gerar o CSR sem o nome alternativo, estes é as instruções para realizar esta tarefa.

Etapa 1. Início de uma sessão a PCP como o usuário de raiz

Etapa 2. Navegue a **/opt/cupm/httpd/ pelo CD /opt/cupm/httpd/ da** entrada

Etapa 3. Tipo: **vi san.cnf**

Note: Isto criará um arquivo novo chamado san.cnf que estará vazio neste momento

Etapa 4. Pressione **I** para a inserção (isto reservará editar o arquivo) e a cópia/pasta o abaixo no campo cinzento

Note por favor também a entrada na parte inferior DNS.1 = pcptest23.cisco.ab.edu é a entrada dos DN principais que será usada para o CSR e o DNS.2 será a secundária; Esta maneira você pode alcançar PCP e usar qualquer uma das entradas de DNS.

Após uma cópia/pasta neste exemplo, remova por favor os exemplos os mais pcptest com esses que você precisa para seu aplicativo.

```
[ 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
```

Etapa 5. Tipo: **o esc** datilografa então**: wq!** (isto salvar o arquivo e as mudanças apenas feitos).

Etapa 6. Serviços do reinício para que o arquivo de configuração tome a influência corretamente. Digite: **parada de /opt/cupm/bin/cpcmcontrol.sh**

o tipo **estado de /opt/cupm/bin/cpcmcontrol.sh** para assegurar todos os serviços parou

Etapa 7. Datilografe este comando permitir que os serviços venham apoio: **começo de /opt/cupm/bin/cpcmcontrol.sh**

Etapa 8. Você deve ainda estar no diretório de **/opt/cupm/httpd/**, você pode datilografar o **pwd** para encontrar seu diretório atual para certificar-se.

Etapa 9. Execute este comando gerar a chave privada e o CSR.

req do OpenSSL - para fora PCPSAN.csr - newkey rsa:2048 - Nós - keyout PCPSAN.key - configuração 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]#
```

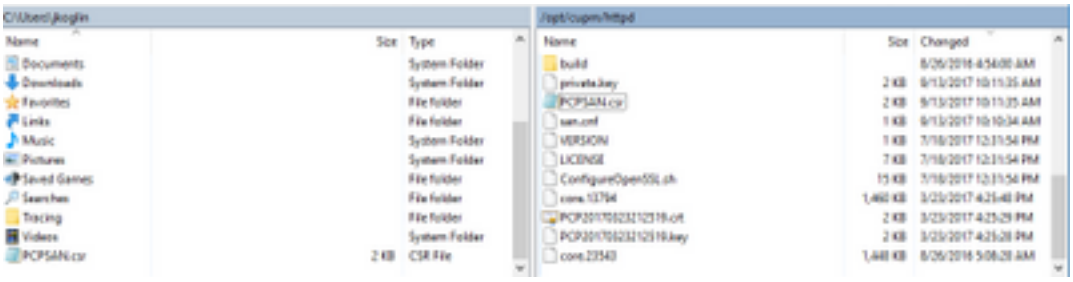
O CSR obtém gerado e para verificar se o CSR contém o tipo correto dos nomes alternativos este comando

req do OpenSSL - noout - texto - em 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**: Se as entradas de DNS são mesma como mostrado abaixo etapa 4, você deve ver o mesmos que você entrou em etapa 4. Depois que você a verifica, continue à próxima etapa

Etapa 10. Use um programa chamado winscp ou o filezilla conecta a PCP como o usuário de raiz e navega ao diretório de **/opt/cupm/httpd/** e move o .csr do server PCP para seu desktop.



Etapa 11. Assine o CSR com seu CA e ou use um Windows Server ou em linha através de um fornecedor de terceira parte tal como DigiCert.

Etapa 12. Instale o certificado PCP no GUI, navegue: **Certificados de Administration>Updates>SSL.**

Etapa 13. Instale o certificado através de seu navegador, referências pelo navegador é como abaixo.

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

Etapa 14. Depois que você instala o certificado no server e em seu navegador, cancele o esconderijo e feche-o fora do navegador.

Etapa 15. Reabra a URL e você não deve encontrar o erro de segurança.

Notas mais adicionais

> Nota: Versão 12.x e mais recente PCP você precisa o TAC de fornecê-lo o acesso CLI enquanto este é restrito.

Processo para pedir o acesso CLI

Etapa 1. Início de uma sessão a PCP GUI

Etapa 2. Navegue a **Administration>Logging e a Showtech>Click no account>create do Troubleshooting o userid** e selecione um período apropriado onde você precisará o acesso raiz de

realizar este.

Etapa 3. Forneça ao TAC a corda do desafio e fornecer-lhe-ão a senha (esta senha será muito longa, não a preocupa trabalhará).

```
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.
```

Etapa 4. Saída de seu usuário atual e início de uma sessão com o userid que você criou e a senha fornecida pelo TAC.

Etapa 5. Navegue a **pesquisar defeitos Account>>Launch>>Click na conta do console** e crie seu usuário CLI - identificação e senha.

Etapa 6. Agora entre a PCP como o usuário que você criou e execute as etapas inicial descritas neste documento.

> Nota: Versão 12.x e mais recente que PCP você precisa de entrar no **sudo do** comando antes de todas as instruções para que trabalhe. Para a etapa 9, o comando consequentemente será **req do OpenSSL do sudo - para fora PCPSAN.csr - o newkey rsa:2048 - Nós - o keyout PCPSAN.key - a configuração san.cnf. Para verificar o** dns você então usaria o sudoopensslreq do comando **- noout - texto - em PCPSAN.csr | grep DNS**