生成CSR用在头等协作供应(PCP)的替代名称指南

目录

简介

本文描述如何生成证书签名请求(CSR)在头等供应允许替代名称。

先决条件

要求

- Certificate Authority (CA)将需要签署您从PCP生成的证书，您能使用Windows服务器或有CA符号它联机。

如果是不确定的如何安排您的证书签字由CA联机资源，请参考下面链路

https://www.digicert.com/

-对头等供应的命令行界面(CLI)的根访问权限将是需要的。根访问权限生成在安装。

> **Note**:PCP版本12.X以上请参考本文的底部在进一步笔记下

使用的组件

头等协作供应

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络实际，请保证您了解所有命令潜在影响。

背景信息

这将允许您访问头等协作供应(PCP)为企业目的与多个域名服务器(DNS)条目使用同一证书和不遇到

验证错误，当您访问网页。

步骤和步骤

在从图形用户界面(GUI)写入的，本文wasw时您能只生成CSR没有替代名称，这些是说明完成此任务。

步骤1. PCP的洛金作为root用户

步骤2.导航对**/opt/cupm/httpd/**由输入**cd /opt/cupm/httpd/**

步骤3.类型： **vi san.cnf**

> **Note**:这将创建呼叫当时将是空的san.cnf的一个新的文件

步骤4.在灰色字段按插入(这将准许编辑文件)和复制/粘贴的**I**下面

请注意在底部的条目DNS.1 = pcptest23.cisco.ab.edu是将使用CSR和DNS.2将是第二的主要的DNS条目;这样您能访问PCP和使用DNS条目之一。

在复制/在本例中后粘贴，请删除与您为您的应用程序需要的那个的pcptest示例。

```
[ 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
```

步骤5.类型：**esc**然后键入**：wq!** (这将保存做的文件和变动)。

步骤6.配置文件的重新启动服务能适当地采取影响。类型： **/opt/cupm/bin/cpcmcontrol.sh终止**

类型保证所有服务的**/opt/cupm/bin/cpcmcontrol.sh状态**终止了

步骤7.键入此命令允许服务恢复：**/opt/cupm/bin/cpcmcontrol.sh开始**

步骤 8您应该仍然是在**/opt/cupm/httpd/**目录，您能键入**pwd**查找您的当前目录确保。

步骤9.运行此命令生成专用密钥和CSR。

openssl req - PCPSAN.csr - newkey rsa:2048 -节点- keyout PCPSAN.key -请配置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]#
```

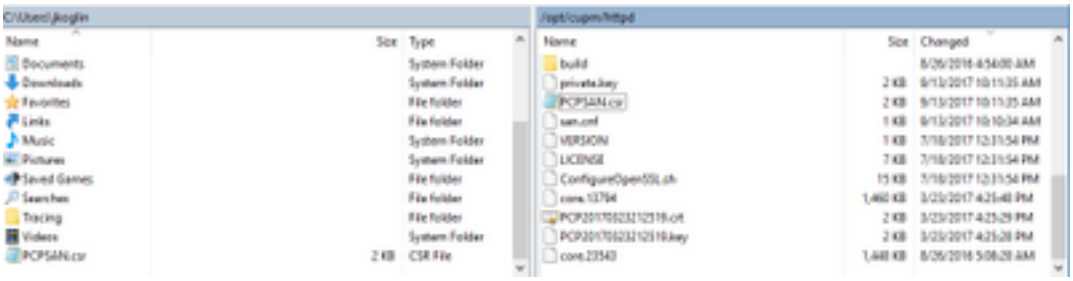
如果CSR包含正确替代名称类型此命令， CSR被生成和验证

openssl req - noout -文本-在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**:如果DNS条目是相同的如下所示步骤4，您应该看到同一样您在步骤4.输入。在您验证它后，请继续对下一步

步骤 10请使用呼叫winscp的一个程序或filezilla连接对PCP作为root用户并且导航对**/opt/cupm/httpd/**目录并且移动从PCP服务器的.csr向您的桌面。



步骤11.签署与您的CA的CSR，并且或者请使用一Windows服务器或联机通过一个第三方供应商例如DigiCert。

步骤 12安装在Gui的PCP证书，导航：**Administration>Updates>SSL证书。**

步骤 13通过您的浏览器安装证书，参考每个浏览器是作为下面。

谷歌镀铬物：

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

步骤 14在您安装在服务器和您的浏览器后的证书，请清除缓存并且关闭在浏览器外面。

步骤 15重新打开URL，并且您不应该遇到安全错误。

进一步笔记

注意：当这限制， PCP版本12.x和以上您需要TAC提供您CLI访问。

请求CLI访问的进程

步骤1. PCP GUI的洛金

步骤2.导航对**Administration>Logging和Showtech>Click在故障排除account>create userid**并且选择您将需要根访问权限完成此的适当时间。

步骤3.提供给TAC挑战字符串，并且他们将提供您密码(此密码将是非常较的，不让它担心将工作)。

```
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.
```

步骤4.您的当前用户和登录注销与userid您已创建和TAC提供的密码。

步骤5.导航对**排除故障在控制台帐户的Account>>Launch>>Click**并且创建您的cli用户ID和密码。

第六步：现在请登陆对PCP作为您创建的用户并且执行描述的初始步骤在本文。

注意：您在命令**sudo**需要输入在它的所有说明之前能工作的PCP版本12.x和以上。因此对于步骤9，命令将是**sudo openssl req - PCPSAN.csr - newkey rsa:2048 -节点- keyout PCPSAN.key -设置san.cnf。要验证**dns您然后会使用命令sudoopensslreq **- noout -文本-在PCPSAN.csr|grep DNS**