إنشاء CSR مع دليل الاسم البديل في إمداد التعاون الأساسي (PCP)

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
الإجراء والخطوات
ملاحظات إضافية

المقدمة

يوضح هذا المستند كيفية إنشاء طلب توقيع شهادة (CSR) في إعداد Prime للسماح بالأسماء البديلة.

المتطلبات الأساسية

المتطلبات

- يجب على "المرجع المصدق" (CA) توقيع الشهادة التي قمت بإنشائها من PCP، ويمكنك إستخدام خادم Windows أو أن توقع عليه من المرجع المصدق عبر الإنترنت.

إذا لم تكن متأكدا من كيفية توقيع شهادتك من قبل أحد موارد المرجع المصدق على الإنترنت، فيرجى الإشارة إلى الارتباط أدناه

/https://www.digicert.com

- يلزم الوصول الجذر إلى واجهة سطر الأوامر (CLI) الخاصة بإمداد Prime. يتم إنشاء الوصول الجذر عند التثبيت.

ملاحظة: بالنسبة لإصدار (إصدارات) PCP 12.x والإصدارات الأعلى، يرجى الرجوع إلى أسفل هذا المستند تحت مزيد من الملاحظات

المكونات المستخدمة

Prime Collaboration Provisioning

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

سيتيح لك ذلك الوصول إلى إمداد التعاون الأساسي (PCP) لأغراض العمل مع إدخالات متعددة لخادم اسم المجال (DNS) باستخدام نفس الشهادة وعدم مواجهة خطأ الشهادة عند الوصول إلى صفحة الويب.

الإجراء والخطوات

في الوقت الذي تمت كتابة هذا المستند، من واجهة المستخدم الرسومية (GUI)، يمكنك إنشاء CSR فقط بدون اسم بديل، وهذه هي التعليمات الخاصة بإنجاز هذه المهمة.

الخطوة 1. تسجيل الدخول إلى PCP كمستخدم جذري

الخطوة 2. انتقل إلى **/opt/cupm/httpd/**بواسطة **القرص المضغوط** الخاص بالإدخال**/opt/cupm/httpd/**

الخطوة 3. النوع: **vi san.cnf**

ملاحظة: سيؤدي هذا إلى إنشاء ملف جديد يسمى san.cnf والذي سيكون فارغا في هذه اللحظة

الخطوة 4. اضغط على **i** للإدراج (الذي سيسمح بتحرير الملف) ونسخ/لصق ما يلي في حقل الرمادي

الرجاء ملاحظة أن الإدخال الموجود في أسفل pcptest23.cisco.ab.edu = DNS.1 هو إدخال DNS الأساسي الذي سيتم إستخدامه ل CSR و DNS.2 سيكون ثانويا؛ بهذه الطريقة يمكنك الوصول إلى PCP واستخدام أي من إدخالات DNS.

بعد نسخ/لصق في هذا المثال، الرجاء إزالة أمثلة PCPPtest مع الأمثلة التي تحتاج إليها للتطبيق.

```
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
```

الخطوة 5. الكتابة: **esc** ثم الكتابة **:wq!** (سيؤدي ذلك إلى حفظ الملف والتغييرات التي تم إجراؤها للتو).

الخطوة 6. قم بإعادة تشغيل الخدمات لتأثير ملف التكوين بشكل صحيح. النوع: **/opt/cupm/bin/cpcmcontrol.sh توقف**

اكتب **/opt/cupm/bin/cpcmcontrol.sh status** لضمان توقف جميع الخدمات

الخطوة 7. اكتب هذا الأمر للسماح للخدمات بالبدء من جديد: **/opt/cupm/bin/cpcmcontrol.shبدء**

الخطوة 8. يجب أن تكون في الدليل **/opt/cupm/httpd/**، يمكنك كتابة **pwd** للعثور على الدليل الحالي للتأكد.

الخطوة 9. قم بتشغيل هذا الأمر لإنشاء المفتاح الخاص و CSR.

openssl req -out pcpsan.csr -new key rsa:2048 -node -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
```

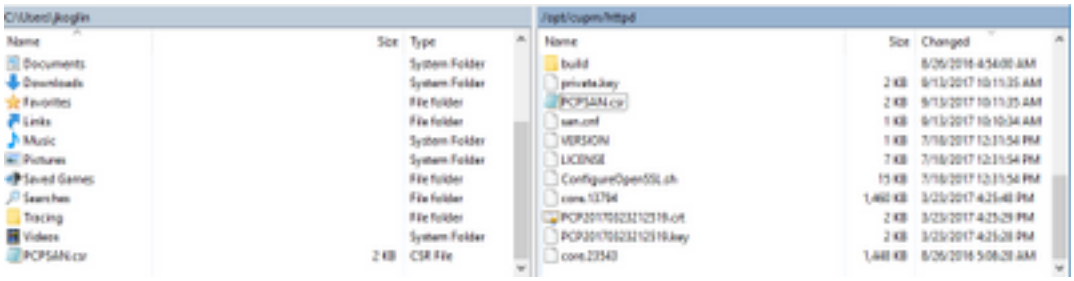
يتم إنشاء CSR والتحقق من إحتواء CSR على نوع الأسماء البديلة الصحيح هذا الأمر

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
```

ملاحظة: إذا كانت إدخالات DNS هي نفسها كما هو موضح أدناه الخطوة 4، فيجب أن ترى نفس الشيء الذي أدخلته في الخطوة 4. بعد التحقق من صحته، انتقل إلى الخطوة التالية

الخطوة 10. أستخدم برنامج يسمى WinSCP أو Filizilla يتصل ب PCP كمستخدم جذري وانتقل إلى دليل **/opt/cupm/httpd/**وانقل csr من خادم PCP إلى سطح المكتب الخاص بك.



الخطوة 11. وقع على CSR مع CA الخاص بك وقم إما باستخدام خادم Windows أو عبر الإنترنت من خلال مورد تابع لجهة خارجية مثل DigiCert.

الخطوة 12. ركبت ال PCP شهادة في ال gui، تنقل: **إدارة>تحديث>SSL شهادة.**

الخطوة 13. قم بتثبيت الشهادة من خلال المستعرض الخاص بك، والمراجع لكل مستعرض كما هي أدناه.

: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

الخطوة 14. بعد تثبيت الشهادة على الخادم والمستعرض، قم بمسح ذاكرة التخزين المؤقت وأغلق المستعرض.

الخطوة 15. أعد فتح عنوان URL ويجب ألا تواجه خطأ الأمان.

ملاحظات إضافية

ملاحظة: PCP صيغة x.12 وأعلى تحتاج TAC أن يوفر لك ال CLI منفذ بما أن هذا يكون مقيد.

معالجة طلب وصول CLI

الخطوة 1. تسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) لبروتوكول PCP

الخطوة 2. انتقل إلى **الإدارة>التسجيل و ShowTech>انقر فوق حساب أستكشاف الأخطاء وإصلاحها>إنشاء معرف المستخدم** وحدد وقتا مناسبا ستحتاج فيه إلى وصول الجذر لتحقيق ذلك.

الخطوة 3. زودت TAC التحدي خيط وهم زودت أنت الكلمة (هذا كلمة يكون طويل جدا، لا تقلق هو سيعمل).

```
: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
```

الخطوة 4. تسجيل الخروج من المستخدم الحالي وتسجيل الدخول باستخدام معرف المستخدم الذي أنشأته وكلمة المرور المقدمة من قبل TAC.

الخطوة 5. انتقل إلى **حساب أستكشاف الأخطاء وإصلاحها>إطلاق>>انقر فوق حساب وحدة التحكم** وقم بإنشاء معرف مستخدم واجهة سطر الأوامر وكلمة المرور الخاصين بك.

الخطوة 6. الآن تسجيل الدخول إلى PCP كالمستخدم الذي أنشأته وأديته الخطوات الأولية المحددة في هذا المستند.

ملاحظة: PCP صيغة x.12 وأعلى تحتاج أن يدخل في الأمر **sudo** قبل كل التعليمات لكي يعمل. للخطوة 9، الأمر لذلك سيكون **- sudo openssl req -out PCPSAN.csr newKey rsa:2048 -node -keyout pcpsan.key -config san.cnf**. للتحقق من الأنظمة الرقمية، يمكنك حينئذ إستخدام الأمر **- sudoopenssl req -noout -text في PCPSAN.csr | GREP DNS**

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).