生成して下さい Prime Collaboration プロビジョニング（PCP）の代替名 ガイドの CSR を

目次

概要

この資料に代替名を可能にする主なプロビジョニングの証明書署名要求（CSR）を生成する方法を記述されています。

前提条件

要件

-認証局（CA）は PCP から生成する認証に署名する必要があります、オンラインそれ Windows サーバを使用するか、または CA サインを持つことができます。

認証を CA オンライン リソースによって署名してもらう方法を不確実下記のリンクを参照して下さい

https://www.digicert.com/

- Prime Provisioning の Command Line Interface（CLI）へのルートアクセスは必要です。 ルートアクセスはインストールに生成されます。

> **注:** PCP に関してはバージョン 12.X はそれ以上のメモの下で以上にこの資料の下部のを示します

使用するコンポーネント

Prime Collaboration Provisioning

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

これは Web ページにアクセスする場合複数の Domain Name Server （DNS）エントリとの Prime Collaboration プロビジョニング（PCP）に同じ認証を使用して業務目的でアクセスし、Certificate エラーに出会わないことを可能にします。

プロシージャおよびステップ

グラフィカル ユーザ インターフェイス（GUI）から、書かれているこの資料 wasw の時に代替名無しでこれらですこのタスクを完了する手順しか CSR を生成できません。

ステップ 1.ルート ユーザとして PCP へのログイン

ステップ 2.入力 **cd /opt/cupm/httpd/** によって **/opt/cupm/httpd/** にナビゲート して下さい

ステップ 3.型: **VI san.cnf**

> **注:** これは今空である san.cnf と呼ばれた新しいファイルを作成します

ステップ 4.挿入（これはファイルを編集することを割り当てます）およびコピー/貼り付けのために灰色フィールドの下記『i』 を押して下さい

以下の事項に注意して下さい:同様に下部ののエントリは DNS.1 = pcptest23.cisco.ab.edu CSR および DNS.2 のためにのセカンダリ使用するプライマリ DNS エントリです; こうすれば PCP にアクセスし、DNS エントリのどちらかを使用できます。

コピーがこの例に/貼り付けた後、アプリケーションのために必要とする物と pcptest 例を取除いて下さい。

```
[ 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
```

ステップ 5.型: **esc はそれから入力します: wq!** と入力し、 （これはちょうど行ったファイルおよび変更を保存します）。

ステップ 6.影響をきちんと奪取 する config ファイルのための再始動 サービス。 Type: **/opt/cupm/bin/cpcmcontrol.sh 停止**

すべてのサービスを確認する型 **/opt/cupm/bin/cpcmcontrol.sh ステータスは**停止しました

ステップ 7.サービスを戻って来ることを許可するようにこのコマンドを入力して下さい: **/opt/cupm/bin/cpcmcontrol.sh 開始する**

ステップ 8 まだ **/opt/cupm/httpd/** ディレクトリに確かめるとワーキング ディレクトリが見つけるように **pwd を**入力できますあるはずです。

ステップ 9.プライベートキーおよび CSR を生成するためにこのコマンドを実行して下さい。

openssl req - PCPSAN.csr - newkey rsa:2048 -ノード- keyout PCPSAN.key -構成 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]#
```

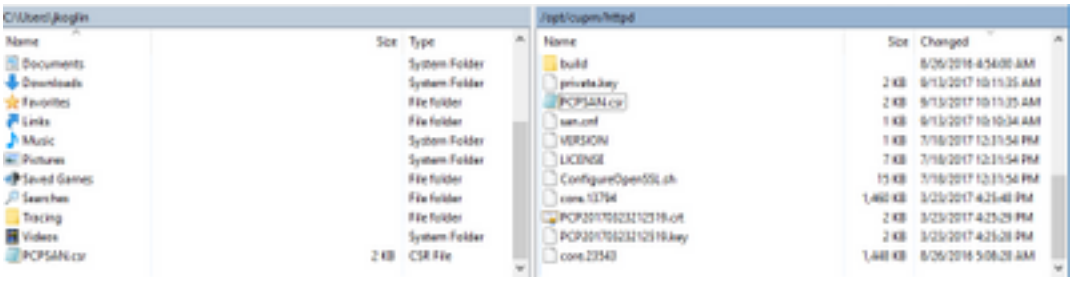
CSR は CSR が正しい代替名型がこのコマンド含まれているかどうか確認するために生成され、

openssl req - noout -テキスト- PCPSAN.csr の… | グレップ 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]#
```

> **注:** DNS エントリがステップ 4 下記に示されているように同じである場合、ステップ 4.で入ったと同じを見るはずです。 それを確認した後、次 の ステップに進んで下さい

ステップ 10 winscp と呼ばれるプログラムを使用すれば filezilla はルート ユーザとして PCP に接続し、**/opt/cupm/httpd/** ディレクトリにナビゲート し、PCP サーバからデスクトップに .csr を移動します。



ステップ 11. CA の CSR に署名すれば DigiCert のようなサードパーティベンダーによって Windows サーバかオンラインを使用して下さい。

手順 12： GUI に PCP 認証を、ナビゲート インストールして下さい: **Administration>Updates>SSL 認証。**

手順 13： ブラウザによって認証を、ブラウザごとの参照あります下記にとしてインストールして下さい。

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

手順 14： サーバおよびブラウザで認証をインストールした後、キャッシュを消去し、ブラウザから閉じて下さい。

手順 15： URL を再開すればセキュリティエラーに出会うべきではありません。

それ以上のメモ

> 注： PCP バージョン 12.x および それ 以上これが制限 されると同時に TAC が CLI アクセスを与えることを必要とします。

CLI アクセスを要求するプロセス

ステップ 1. PCP GUI へのログイン

ステップ 2.**トラブルシューティング account>create の Administration>Logging および Showtech>Click** へのナビゲートは **USERID** およびルートアクセスがこれを達成することを必要とする適切な時間を選択します。

ステップ 3. TAC にチャレンジ ストリングを提供し、それらはパスワードを提供します（このパスワードは非常に長かったり、それをはたらきます心配しません）。

```
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.
```

ステップ 4.現在のユーザのログアウトおよびおよび TAC によって提供されたパスワード作成した USERID のログオン。

ステップ 5.**コンソール アカウントの Account>>Launch>>Click の解決**へのナビゲートは cli ユーザー ID およびパスワードを作成し。

ステップ 6 作成したログインし、この資料に説明がある第 一歩を実行して下さいユーザようにこの場合 PCP に。

> 注： はたらくそれのためのすべての指示前にコマンド **sudo** で入力する必要がある PCP バージョン 12.x および それ 以上。 従ってステップ 9 に関しては、コマンドは **sudo openssl req - PCPSAN.csr - newkey rsa:2048 -ノード- keyout PCPSAN.key -構成 san.cnf** です。 dns を**確認するために- PCPSAN.csr の…**それからコマンド sudoopensslreq を**- noout -テキスト**使用します **| グレップ DNS**