Генерируйте CSR с руководством альтернативного названия в Главной инициализации совместной работы (PCP)

Содержание

Введение

Этот документ описывает, как генерировать Запрос подписи сертификата (CSR) в главной инициализации для учета альтернативных названий.

Предварительные условия

Требования

- Центр сертификации (CA) должен будет подписать сертификат, который вы генерируете от PCP, можно использовать Windows Server или иметь знак CA это онлайн.

Если вы не уверены, как подписать ваш Сертификат CA онлайновый ресурс, сошлитесь на ссылку ниже

https://www.digicert.com/

- Доступ к корневому каталогу к Интерфейсу командной строки (CLI) Главной Инициализации будет необходим. Доступ к корневому каталогу генерируется после Установки.

> **Примечание:** Для Версии (версий) 12. X PCP и выше см. нижнюю часть этого документа под Дальнейшими Примечаниями

Используемые компоненты

Главная инициализация совместной работы

Сведения, представленные в этом документе, были получены от устройств, работающих в

специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, гарантируйте понимание потенциального воздействия любой команды.

Общие сведения

Это позволит вам обращаться к Главной инициализации совместной работы (PCP) для бизнес-целей с Сервером имен составного домена (DNS) записи с помощью того же сертификата и не встречаться с ошибкой сертификата при доступе к веб-странице.

Процедура и шаги

Во время этого документа wasw записанный, от Графического пользовательского интерфейса (GUI) можно только генерировать CSR без альтернативного названия, Это инструкции для выполнения этой задачи.

Шаг 1. Войдите к PCP как пользователь маршрута

Шаг 2. Перейдите к**/opt/cupm/httpd/** входным **CD/opt/cupm/httpd/**

Шаг 3. Введите : **vi san.cnf**

> **Примечание:** Это создаст новый файл, названный san.cnf, который будет пуст в данный момент

Шаг 4. . Потребуйте **y l** вставки (это позволит редактировать файл), и скопировать/вставить ниже в сером поле

Обратите внимание также на запись в нижнем Dns 1 = pcptest23. cisco . ab.edu является основная Запись DNS, которая будет использоваться для CSR, и Dns 2 будет вторичным устройством; Таким образом, можно обратиться к PCP и использовать любую из Записей DNS.

После скопировать/вставить в данном примере, удалите pcptest примеры с теми, вам нужно для вашего приложения.

```
[ 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
```

Шаг 5. . Введите : **esc** тогда вводят **: wq!** (это сохранит файл и изменения, просто внесенные).

Шаг 6. Сервисы перезапуска для файла config для взятия влияния должным образом. Введите : **/opt/cupm/bin/cpcmcontrol.sh останавливаются**

введите **/opt/cupm/bin/cpcmcontrol.sh статус**, чтобы гарантировать, что остановились все сервисы

Шаг 7. Введите эту команду, чтобы позволить сервисам возвращаться:**/opt/cupm/bin/cpcmcontrol.sh запускаются**

Шаг 8. Необходимо все еще быть в**/opt/cupm/httpd/**каталоге, можно ввести **pwd**, чтобы найти, что удостоверяется текущий каталог.

Шаг 9. Выполните эту команду для генерации Секретного ключа и CSR.

req openssl - PCPSAN.csr-newkey rsa:2048 - узлы-keyout private.key - конфигурирует 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]#
```

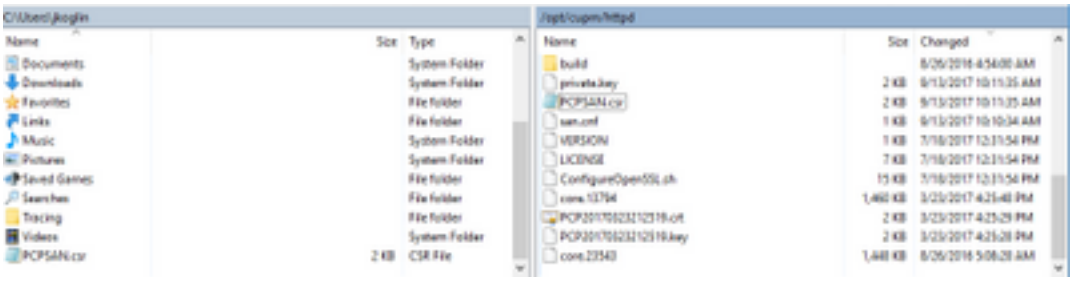
CSR генерируется и проверить, содержит ли CSR корректный тип Альтернативных названий эта команда

req openssl-noout - текст - в PCPSAN.csr | DNS grep

```
[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]#
```

> **Примечание:** Если Записи DNS совпадают с показанный ниже шага 4, необходимо видеть то же, когда вы ввели в шаге 4. После того, как вы проверяете его, продолжаетесь к следующему шагу

Шаг 10. Используйте программу, названную winscp, или filezilla соединяются с PCP как пользователь маршрута и перешли к**/opt/cupm/httpd/**каталогу и перемещают .csr от сервера PCP до вашего рабочего стола.



Шаг 11. Подпишите CSR со своим CA и или используйте Windows Server или онлайн через стороннего поставщика, такого как DigiCert.

Шаг 12. Установите Сертификат PCP в Gui, Перейдите: **Администрирование> Обновления> сертификаты SSL.**

Шаг 13. Установите сертификат через свой браузер, ссылки на браузер как ниже.

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

Шаг 14. После установки сертификата на сервере и браузере очистите кэш и близко из браузера.

Шаг 15. Вновь откройте URL, и вы не должны встречаться с ошибкой системы безопасности.

Дальнейшие примечания

> Примечание: Версия 12.x PCP и выше вас TAC потребности для предоставления вам доступ CLI, поскольку это ограничено.

Процесс для запроса доступа CLI

Шаг 1. Войдите к GUI PCP

Шаг 2. Перейдите к **администрированию>, Logging и Showtech> Щелкают по учетной записи устранения проблем>, создают идентификатор пользователя** и выбирают подходящее время, вам будет нужен доступ к корневому каталогу для выполнения этого.

Шаг 3. Предоставьте TAC строку проблемы, и они предоставят вас пароль (этот пароль будет очень длинен, не волнуйтесь, что это будет работать).

```
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.
```

Шаг 4. . Выход из системы вашего текущего пользователя и вход в систему с идентификатором пользователя вы создали и пароль, предоставленный TAC.

Шаг 5. . Перейдите к **Устранению проблем Учетной записи>>, Запуск>> Щелкает по Console Account** и создает ваш идентификатор пользователя CLI и пароль.

Шаг 6. Теперь вход в систему к PCP как пользователь вы создали, и выполните первые шаги, описанные в этом документе.