Резервное копирование и восстановаления примера конфигурации сервера IOS CA

Содержание

Введение

Этот документ описывает, как резервировать и восстановить сервер IOS® Certificate Authority (CA) для программного обеспечения Cisco IOS.

См. Настраивают и Регистрируют Cisco VPN 3000 Concentrator к маршрутизатору Cisco IOS как Сервер CA, чтобы узнать больше, как настроить маршрутизатор Cisco IOS как сервер CA.

Предварительные условия

Требования

Запланируйте свой PKI перед Настройкой сервера сертификатов

Перед настройкой сервера сертификатов Cisco IOS важно, чтобы вы запланировали и выбрали соответствующие значения для параметров настройки, которые вы намереваетесь использовать в вашем PKI (таком как сроки службы сертификата и сроки службы списка отозванных сертификатов (CRL)). После того, как параметры настройки настроены в сервере сертификатов, и сертификаты предоставляют, настройки не могут быть изменены, не имея необходимость реконфигурировать сервер сертификатов и повторно регистрируя узлы. Для получения информации о настройках по умолчанию сервера сертификатов и рекомендуемых настройках, обратитесь к Значениям по умолчанию Сервера сертификатов и Рекомендуемым значениям.

Включение сервера HTTP

Сервер сертификатов поддерживает Протокол SCEP (SCEP) по HTTP. Сервер HTTP должен быть позволен на маршрутизаторе для сервера сертификатов использовать SCEP. (Для включения сервера HTTP используйте **команду ip http server**.) Сервер сертификатов автоматически включает или отключает сервисы SCEP после того, как сервер HTTP будет включен или отключен. Если сервер HTTP не включен, только регистрация руководства PKCS10 поддерживается.

Надежные сервисы времени

Сервисы времени должны работать на маршрутизаторе, потому что сервер сертификатов должен иметь надежное знание времени. Если аппаратные часы недоступны, сервер сертификатов зависит от вручную параметров настройки настроенной синхронизации, таких как Протокол NTP. См. раздел Setting Time and Calendar Services Руководства по конфигурации Основных принципов Конфигурации Cisco IOS для получения дополнительной информации о NTP. Если нет аппаратных часов, или часы недопустимы, это индикаторы сообщения в загрузке:

```
% Time has not been set. Cannot start the Certificate server.
```

После того, как часы установлены, сервер сертификатов автоматически переключается на рабочий статус.

Используемые компоненты

Сведения в этом документе основываются на Маршрутизаторе Cisco 3600 с Cisco IOS Software Release 12.4 (8).

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Резервируйте IOS CA сервер

При начальной настройке сервера сертификатов можно позволить сертификату CA и ключу CA быть автоматически заархивированным так, чтобы они могли быть восстановлены позже, если потеряны или оригинал или оригинальная конфигурация.

Когда сервер сертификатов включен первоначально, сертификат CA, и CA ключ генерируется. Если автоматический архив также включен, сертификат CA и ключ CA экспортируются (заархивированные) в базу данных сервера. Архив может быть в формате Privacy Enhanced Mail (PEM) или PKCS12.

Примечание:

- Этот резервный файл ключа CA чрезвычайно важен и должен быть сразу перемещен в другое защищенное место.
- Это действие архивации происходит только в один раз. Только ключ CA, который вручную генерируется и отмечается экспортный или автоматически генерируемый сервером сертификатов, заархивирован (этот ключ отмечен неэкспортный).
- Автоархивация не происходит, если вы генерируете ключ CA вручную и отмечаете его "неэкспортный".
- В дополнение к сертификату CA и CA ключевому архивному файлу, необходимо также регулярно выполнять резервное копирование последовательный файл (.ser) и файл CRL (.crl). Если необходимо восстановить сервер сертификатов, последовательный файл и файл CRL оба важны для операции CA.

Примечание: Не возможно вручную выполнить резервное копирование сервер, который использует неэкспортные ключи RSA или вручную генерировал неэкспортные ключи RSA. Несмотря на то, что автоматически генерируемые ключи RSA отмечены как неэкспортные, они автоматически заархивированы однажды.

Пример:

- **Формат PEM** — Создает CA и резервирует файлы от энергонезависимой памяти (NVRAM) (к серверу TFTP в этом случае):

```
!--- Create a server named CA. Router(config)#crypto pki server CA
!--- Archive in the PEM format with the encryption key as cisco123. Router(cs-
server)#database archive pem password cisco123
!--- Lifetime of the certificates issued by this certificate server in days. Router(cs-
server)#lifetime certificate 1095
!--- Lifetime of the certificate server signing certificate in days. Router(cs-
server)#lifetime ca-certificate 1825
!--- Lifetime of the CRLs published by this certificate server in hours. Router(cs-
server)#lifetime crl 24
Router(cs-server)#no shutdown

%Some server settings cannot be changed after CA certificate generation.
% Generating 1024 bit RSA keys, keys will be non-exportable...
Feb 21 17:39:36.916: crypto_engine: generate public/private keypair [OK]
Feb 21 17:39:48.808: crypto_engine: generate public/private keypair
Feb 21 17:39:48.812: %SSH-5-ENABLED: SSH 1.99 has been enabled
Feb 21 17:39:48.812: crypto_engine: public key sign % Exporting
Certificate Server signite and keys...

% Certificate Server enabled.
Router(cs-server)#
Feb 21 17:39:54.064: crypto_engine: public key verify

Router#dir nvram:
Directory of nvram:/

!--- Output is suppressed.     6  -rw-          32                    <no date>  CA.ser
    7  -rw-         212                    <no date>  CA.crl
    8  -rw-        1702                    <no date>  CA.pem
```

```
129016 bytes total (116676 bytes free)

!--- Backup the three files to the TFTP server. Router#copy nvram:CA.ser
tftp://172.16.1.100/backup.ser
Router#copy nvram:CA.crl tftp://172.16.1.100/backup.crl
Router#copy nvram:CA.pem tftp://172.16.1.100/backup.pem
```

- **Формат PKCS12** — Создает CA и резервирует файлы от NVRAM (к серверу TFTP в этом случае).
```
Router (config)#crypto pki server CA
Router (cs-server)#database archive pkcs12 password cisco123
Router(cs-server)#lifetime certificate 1095
Router(cs-server)#lifetime ca-certificate 1825
Router(cs-server)#lifetime crl 24
Router(cs-server)#no shutdown
% Generating 1024 bit RSA keys ...[OK]
% Ready to generate the CA certificate.
% Some server settings cannot be changed after CA certificate generation.
Are you sure you want to do this? [yes/no]: y
% Exporting Certificate Server signing certificate and keys...
! Note that you are not being prompted for a password.
% Certificate Server enabled.
Router (cs-server)# end
Router#dir nvram:
Directory of nvram:/
   125   -rw-         1693            <no date>   startup-config
   126   ----            5            <no date>   private-config
     1   -rw-           32            <no date>   CA.ser
     2   -rw-          214            <no date>   CA.crl
!--- Note that the next line indicates that the format is PKCS12.  3   -rw-         1499
<no date>   CA.p12

Router#copy nvram:CA.ser tftp://172.16.1.100/backup.ser
Router#copy nvram:CA.crl tftp://172.16.1.100/backup.crl
Router#copy nvram:CA.p12 tftp://172.16.1.100/backup.p12
```

Восстановите IOS CA сервер

Для восстановления сервера CA необходимо восстановить **.ser** и **.crl** файлы, воссоздать сервер и импортировать данные из файла PEM (формат PEM) или p12 файла (формат PKCS12).

В нашем лабораторном сценарии **команда no crypto pki server CA** используется для удаления конфигурации сервера сертификатов из маршрутизатора.

Пример:

- **Формат PEM** — Позволяет вам просматривать файл PEM так, чтобы можно было скопировать и вставить сертификат и ключ позже использование **команды more CA.pem**.Данный пример показывает, что восстановление от архива PEM и что database URL является nvram:
```
Router#copy tftp://172.16.1.100/backup.ser nvram:CA.ser
Destination filename [CA.ser]?
32 bytes copied in 1.320 secs (24 bytes/sec)
Router#copy tftp://172.16.1.100/backup.crl nvram:CA.crl
Destination filename [CA.crl]?
214 bytes copied in 1.324 secs (162 bytes/sec)
Router#configure terminal
!--- Because the CA certificate has digital signature usage, you need to !--- import using
the "usage-keys" keyword. !--- This is the command you use to import the certificate !---
via the terminal with encryption key cisco123. Router (config)#crypto ca import CA pem
```

```
usage-keys terminal cisco123
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.
 !--- Copy and paste the CERTIFICATE from the pem file, !--- followed by quit.

-----BEGIN CERTIFICATE-----
MIIB9zCCAWCgAwIBAgIBATANBgkqhkiG9w0BAQQFADAPMQ0wCwYDVQQDEwRteWNz
MB4XDTA0MDkwMjIxMDI1NloXDTA3MDkwMjIxMDI1NlowDzENMAsGA1UEAxMEbXlj
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuGnnDXJbpDDQwCuKGs5Zg2rc
K7ZJauSUotTmWYQvNx+ZmWrUs5/j9Ee5FV2YonirGBQ9mc6u163kNlrIPFck062L
GpahBhNmKDgod1o2PHTnRlZpEZNDIqU2D3hACgByxPjrY4vUnccV36ewLnQnYpp8
szEu7PYTJr5dU5ltAekCAwEAAaNjMGEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8B
Af8EBAMCAYYwHwYDVR0jBBgwFoAUaEEQwYKCQ1dm9+wLYBKRTlzxaDIwHQYDVR0O
BBYEFGhBEMGCgkNXZvfsC2ASkU5c8WgyMA0GCSqGSIb3DQEBBAUAA4GBAHyhiv2C
mH+vswkBjRA1Fzzk8ttu9s5kwqG0dXp25QRUWsGlr9nsKPNdVKt3P7p0A/KochHe
eNiygiv+hDQ3FVnzsNv983le6O5jvAPxc17RO1BbfNhqvEWMsXdnjHOcUy7XerCo
+bdPcUf/eCiZueH/BEy/SZhD7yovzn2cdzBN
-----END CERTIFICATE-----
quit
!--- Copy and paste the PRIVATE KEY from the pem file, !--- followed by quit.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,5053DC842B04612A
1CnlF5Pqvd0zp2NLZ7iosxzTy6nDeXPpNyJpxB5q+V29IuY8Apb6TlJCU7YrsEB/
nBTK7K76DCeGPlLpcuyEI171QmkQJ2gA0QhC0LrRo09WrINVH+b4So/y7nffZkVb
p2yDpZwqoJ8cmRH94Tie0YmzBtEh6ayOud11z53qbrsCnfSEwszt1xrW1MKrFZrk
/fTy6loHzGFzl3BDj4r5gBecExwcPp74ldHO+Ld4Nc9egG8BYkeBCsZZOQNVhXLN
I0tODOs6hP915zb6OrZFYv0NK6grTBO9D8hjNZ3U79jJzsSP7UNzIYHNTzRJiAyu
i56Oy/iHvkCSNUIK6zeIJQnW4bSoM1BqrbVPwHU6QaXUqlNzZ8SDtw7ZRZ/rHuiD
RTJMPbKquAzeuBss1132OaAUJRStjPXgyZTUbc+cWb6zATNws2yijPDTR6sRHoQL
47wHMr2Yj80VZGgkCSLAkL88ACz9TfUiVFhtfl6xMC2yuFl+WRk1XfF5VtWe5Zer
3Fn1DcBmlF7O86XUkiSHP4EV0cI6n5ZMzVLx0XAUtdAl1gD94y1V+6p9PcQHLyQA
pGRmj5IlSFw90aLafgCTbRbmC0ChIqHy91UFa1ub0130+yu7LsLGRlPmJ9NE61JR
bjRhlUXItRYWY7C4M3m/0wz6fmVQNSumJM08RHq6lUB3olzIgGIZlZkoaESrLG0p
qq2AENFemCPF0uhyVS2humMHjWuRr+jedfc/IMl7sLEgAdqCVCfV3RZVEaNXBud1
4QjkuTrwaTcRXVFbtrVioT/puyVUlpA7+k7w+F5TZwUV08mwvUEqDw==
-----END RSA PRIVATE KEY-----
quit

!--- Copy and paste again the CERTIFICATE from the pem file, !--- followed by quit.
-----BEGIN CERTIFICATE-----
MIIB9zCCAWCgAwIBAgIBATANBgkqhkiG9w0BAQQFADAPMQ0wCwYDVQQDEwRteWNz
MB4XDTA0MDkwMjIxMDI1NloXDTA3MDkwMjIxMDI1NlowDzENMAsGA1UEAxMEbXlj
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuGnnDXJbpDDQwCuKGs5Zg2rc
K7ZJauSUotTmWYQvNx+ZmWrUs5/j9Ee5FV2YonirGBQ9mc6u163kNlrIPFck062L
GpahBhNmKDgod1o2PHTnRlZpEZNDIqU2D3hACgByxPjrY4vUnccV36ewLnQnYpp8
szEu7PYTJr5dU5ltAekCAwEAAaNjMGEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8B
Af8EBAMCAYYwHwYDVR0jBBgwFoAUaEEQwYKCQ1dm9+wLYBKRTlzxaDIwHQYDVR0O
BBYEFGhBEMGCgkNXZvfsC2ASkU5c8WgyMA0GCSqGSIb3DQEBBAUAA4GBAHyhiv2C
mH+vswkBjRA1Fzzk8ttu9s5kwqG0dXp25QRUWsGlr9nsKPNdVKt3P7p0A/KochHe
eNiygiv+hDQ3FVnzsNv983le6O5jvAPxc17RO1BbfNhqvEWMsXdnjHOcUy7XerCo
+bdPcUf/eCiZueH/BEy/SZhD7yovzn2cdzBN
-----END CERTIFICATE-----
quit
!--- When you are prompted for the encryption key, !--- enter quit to skip this step.
quit


Router (config)#crypto pki server CA
Router (cs-server)#database url nvram:
!--- Fill in any CS configuration here. Router (cs-server)#no shutdown
% Certificate Server enabled.
Router (cs-server)#end
```

```
Router#show crypto pki server
Certificate Server CA:
    Status: enabled
    Server's current state: enabled
    Issuer name: CN=CA
    CA cert fingerprint: F04C2B75 E0243FBC 19806219 B1D77412
    Granting mode is: manual
    Last certificate issued serial number: 0x2
    CA certificate expiration timer: 21:02:55 GMT Sep 2 2007
    CRL NextUpdate timer: 21:02:58 GMT Sep 9 2004
    Current storage dir: nvram:
Database Level: Minimum - no cert data written to storage
```

- **Формат PKCS12** — Данный пример показывает, что восстановление от архива PKCS12 и что database URL является NVRAM (по умолчанию).

```
Router#copy tftp://172.16.1.100/backup.ser nvram:CA.ser
Destination filename [CA.ser]?
32 bytes copied in 1.320 secs (24 bytes/sec)
Router#copy tftp://172.16.1.100/backup.crl nvram:CA.crl
Destination filename [CA.crl]?
214 bytes copied in 1.324 secs (162 bytes/sec)
Router#configure terminal
Router (config)#crypto pki import CA pkcs12 tftp://172.16.1.100/backup.p12
              cisco123
Source filename [backup.p12]?
CRYPTO_PKI: Imported PKCS12 file successfully.

Router (config)#crypto pki server CA
!--- Fill in any CS configuration here. Router (cs-server)#no shutdown
% Certificate Server enabled.
Router (cs-server)#end
Router#show crypto pki server
Certificate Server CA:
    Status: enabled
    Server's current state: enabled
    Issuer name: CN=CA
    CA cert fingerprint: 34885330 B13EAD45 196DA461 B43E813F
    Granting mode is: manual
    Last certificate issued serial number: 0x1
    CA certificate expiration timer: 01:49:13 GMT Aug 28 2007
    CRL NextUpdate timer: 01:49:16 GMT Sep 4 2004
    Current storage dir: nvram:
    Database Level: Minimum - no cert data written to storage
```

Проверка

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Команда show crypto pki server показывает информацию о сервере сертификации.

```
Router#show crypto pki server
Certificate Server CA:
    Status: enabled
    Server's current state: enabled
    Issuer name: CN=CA
    CA cert fingerprint: F04C2B75 E0243FBC 19806219 B1D77412
    Granting mode is: manual
    Last certificate issued serial number: 0x2
    CA certificate expiration timer: 21:02:55 GMT Sep 2 2007
```

```
    CRL NextUpdate timer: 21:02:58 GMT Sep 9 2004
    Current storage dir: nvram:
Database Level: Minimum - no cert data written to storage
```

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Поддержка продуктов безопасности маршрутизатора
- Настройка и управление сервером сертификатов Cisco IOS для развертываний PKI
- Cisco Systems – техническая поддержка и документация