Alternativo e restauração um exemplo de configuração de servidor IO CA

Índice

Introdução

Este documento descreve como a alternativo e à restauração um server do Certificate Authority (CA) IOS® para o Cisco IOS Software.

Consulte para configurar e registrar um Cisco VPN 3000 Concentrator a um roteador do Cisco IOS como um server de CA a fim aprender mais sobre como configurar um roteador do Cisco IOS como um server de CA.

Pré-requisitos

Requisitos

Planeie seu PKI antes que você configure o servidor certificado

Antes que você configure um servidor certificado do Cisco IOS, é valores apropriados importantes que você planejou para e escolhidos para os ajustes que você pretende se usar dentro de seu PKI (tal como vidas do certificado e vidas do Certificate Revocation List (CRL)). Depois que os ajustes estão configurados no servidor certificado e os Certificados estão concedidos, os ajustes não podem ser mudados sem ter que reconfigurar o servidor certificado e re-registrar os pares. Para obter informações sobre das configurações padrão e das configurações recomendadas do servidor certificado, refira valores padrão e valores recomendados do servidor certificado.

Habilite o servidor de HTTP

O servidor certificado apoia o protocolo simple certificate enrollment (SCEP) sobre o HTTP. O

Server do HTTP deve ser permitido no roteador para que o servidor certificado use o SCEP. (A fim permitir o Server do HTTP, use o **comando ip http server**.) O servidor certificado permite automaticamente ou os serviços das inutilizações SCEP após o Server do HTTP são permitidos ou desabilitados. Se o Server do HTTP não é permitido, simplesmente o registro PKCS10 manual está apoiado.

Time Services seguro

O Time Services deve ser executado no roteador porque o servidor certificado deve ter o conhecimento seguro do tempo. Se um relógio de hardware é não disponível, o servidor certificado depende manualmente dos ajustes do relógio configurado, tais como o Network Time Protocol (NTP). Refira a época do ajuste e a seção dos serviços do calendário do manual de configuração das configurações fundamentais de IOS Cisco para obter mais informações sobre do NTP. Se não há um relógio de hardware ou o pulso de disparo é inválido, este exibições de mensagem na inicialização:

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

Depois que o pulso de disparo é ajustado, o servidor certificado comuta automaticamente a estado running.

Componentes Utilizados

A informação neste documento é baseada no Cisco 3600 Router com Cisco IOS Software Release 12.4(8).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Backup o server IO CA

Na instalação inicial do servidor certificado, você pode permitir o certificado de CA e a chave de CA a ser arquivado automaticamente de modo que possam ser restaurados mais tarde se a cópia original ou a configuração original são perdidas.

Quando o servidor certificado é girado sobre a primeira vez, o certificado de CA e a chave de CA

estão gerados. Se o arquivo automático é permitido igualmente, o certificado de CA e a chave de CA estão exportados (arquivado) para a base de dados do servidor. O arquivo pode estar no PKCS12 ou no formato do Privacy Enhanced Mail (PEM).

Nota:

- Este arquivo de backup da chave de CA é extremamente importante e deve ser movido imediatamente para um outro lugar fixado.
- Esta ação de arquivística ocorre somente uma vez. Somente a chave de CA que é gerada manualmente e exportable marcado ou gerada automaticamente pelo servidor certificado é arquivada (esta chave é NON-exportable marcado).
- Auto-arquivístico não ocorre se você gerencie a chave de CA manualmente e a marca “NON-exportable.”
- Além do que o certificado de CA e o arquivo morto chave de CA, você deve igualmente regularmente suportar o arquivo de série (.ser) e o arquivo CRL (.crl). O arquivo de série e o arquivo CRL são ambo o críticos para a operação de CA se você precisa de restaurar seu servidor certificado.

Nota: Não é possível suportar manualmente um server que as chaves NON-exportable dos usos RSA ou RSA NON-exportable manualmente gerado fechem. Embora as chaves automaticamente geradas RSA sejam marcadas como NON-exportable, são arquivadas automaticamente uma vez.

Exemplo:

- **Formato PEM** — Crie CA e o backup os arquivos do RAM não-volátil (NVRAM) (ao servidor TFTP neste caso):

```
!--- 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
```

- **Formato do PKCS12** — Crie CA e o backup os arquivos do NVRAM (ao servidor TFTP neste caso).

```
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
```

Restaure o server IO CA

A fim restaurar o server de CA, você precisa de restaurar os arquivos **.ser** e **.crl**, para recrear o server, e para importar os dados do PEM arquive (formato PEM) ou o arquivo p12 (formato do PKCS12).

Em nosso cenário de laboratório, **nenhum** comando **cripto de CA do server do pki** é usado remover a configuração de servidor certificado do roteador.

Exemplo:

- **Formato PEM** — Permite que você ver o arquivo PEM de modo que você possa copiar e colar o certificado e o fechar mais tarde usando **mais comando CA.pem**.Este exemplo mostra que a restauração é de um arquivo PEM e que o base de dados URL é 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
```

- **Formato do PKCS12** — Este exemplo mostra que a restauração é de um arquivo do PKCS12 e que o base de dados URL é NVRAM (o padrão).

```
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
```

Verificar

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

O comando show crypto pki server mostra a informação sobre o server da certificação.

```
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
```

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Sustentação do produto da Segurança de roteadores
- Configurando e controlando um servidor certificado do Cisco IOS para o desenvolvimento PKI
- Suporte Técnico e Documentação - Cisco Systems