Contenido

Introducción

Este documento describe cómo a de reserva y al restore un servidor del Certificate Authority (CA) IOS® para el Cisco IOS Software.

Refiera a la configuración y aliste un Cisco VPN 3000 Concentrator a un router del Cisco IOS como un servidor de CA para aprender más sobre cómo configurar a un router del Cisco IOS como servidor de CA.

prerrequisitos

Requisitos

Planee su PKI antes de que usted configure al servidor de certificados

Antes de que usted configure a un servidor de certificados del Cisco IOS, es valores apropiados importantes que usted ha planeado para y elegidos para las configuraciones que usted se prepone utilizar dentro de su PKI (tal como cursos de la vida del certificado y cursos de la vida del Listas de revocación de certificados (CRL)). Después de que las configuraciones se configuren en el servidor de certificados y se conceden los Certificados, las configuraciones no pueden ser cambiadas sin tener que configurar de nuevo el servidor de certificados y re-alistar a los pares. Para la información sobre las configuraciones predeterminadas y las configuraciones recomendadas del servidor de certificados, refiera a los valores predeterminados y a los valores recomendados del servidor de certificados.

Habilite el servidor HTTP

El servidor de certificados soporta el protocolo simple certificate enrollment (SCEP) sobre el HTTP. El servidor HTTP debe ser habilitado en el router para que el servidor de certificados utilice el SCEP. (Para habilitar al servidor HTTP, utilice el **comando ip http server**.) El servidor de certificados habilita automáticamente o habilitan o se inhabilitan a los servicios de las neutralizaciones SCEP después del servidor HTTP. Si no habilitan al servidor HTTP, sólo se soporta la inscripción manual PKCS10.

Servicios de tiempo confiables

Los Servicios de tiempo deben ejecutarse en el router porque el servidor de certificados debe tener conocimiento confiable del tiempo. Si un reloj de hardware es inasequible, el servidor de certificados depende manualmente de las configuraciones del reloj configurado, tales como Network Time Protocol (NTP). Refiera a la época de la configuración y a la sección de los servicios del calendario de la guía de configuración de los fundamentales de la configuración del Cisco IOS para más información sobre el NTP. Si no hay un reloj de hardware o el reloj es inválido, este las presentaciones del mensaje en el bootup:

Después de que se fije el reloj, del servidor de certificados el Switches automáticamente al estatus corriente.

Componentes Utilizados

La información en este documento se basa en el Cisco 3600 Router con el Cisco IOS Software Release 12.4(8).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Respaldo el servidor IOS CA

En la configuración inicial del servidor de certificados, usted puede habilitar el certificado de CA y la clave de CA que se archivará automáticamente para poderlos restablecer más adelante si se pierde la copia original o la configuración de origen.

Cuando giran al servidor de certificados la primera vez, se generan el certificado de CA y la clave de CA. Si el archivo automático también se habilita, el certificado de CA y la clave de CA se exporta (archivado) a la base de datos del servidor. El archivo puede estar en el PKCS12 o el formato del Privacy Enhanced Mail (PEM).

Nota:

- Este archivo de backup de la clave de CA es extremadamente importante y se debe mover inmediatamente a otro lugar asegurado.
- Esta acción que archiva ocurre solamente una vez. Solamente la clave de CA que es

generada manualmente y exportable marcada o generada automáticamente por el servidor de certificados está archivada (esta clave es NON-exportable marcado).
- Auto-archival no ocurre si usted genera la clave de CA manualmente y la marca “NON-exportable.”
- Además del certificado de CA y del archivo dominante de CA, usted debe también sostener regularmente el archivo serial (.ser) y el archivo CRL (.crl). El archivo serial y el archivo CRL son críticos para el funcionamiento de CA si se necesita restablecer el servidor de certificados.

Nota: No es posible sostener manualmente un servidor que las claves NON-exportables de las aplicaciones RSA o RSA NON-exportable manualmente generado cierren. Aunque las claves automáticamente generadas RSA se marquen como NON-exportable, están archivadas automáticamente una vez.

Ejemplo:

- ¿**Formato PEM**? Cree CA y el respaldo los archivos del RAM no volátil (NVRAM) (al servidor TFTP en este 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 keypairFeb 21 17:39:48.812: %SSH-5-ENABLED: SSH 1.99 has been enabledFeb 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 verifyRouter#**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 del PKCS12**? Cree CA y el respaldo los archivos del NVRAM (al servidor TFTP en este 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)# endRouter#**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**

Restablezca el servidor IOS CA

Para restablecer el servidor de CA, usted necesita restablecer los archivos **.ser** y **.crl**, reconstruir el servidor, e importar los datos del PEM clasifíe (formato PEM) o el archivo p12 (formato del PKCS12).

En nuestro escenario de laboratorio, no se utiliza el **ningún** comando **crypto de CA del servidor pki** de quitar la configuración de servidor de certificados del router.

Ejemplo:

- **¿Formato PEM**? Permite que usted vea el archivo PEM de modo que usted pueda copiar y pegar el certificado y cerrarlo más adelante usando el **más comando CA.pem**.Este ejemplo muestra que la restauración es de un archivo PEM y que la base de datos URL es 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-----
MIIB9zCCAWCgAwIBAgIBATANBgkqhkiG9w0BAQQFADAPMQ0wCwYDVQQDEwRteWNzMB4XDTA0MDkwMjIxMDI1NloXDTA3MDkwMjIxMDI1NlowDzENMAsGA1UEAxMEbXljczCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuGnnDXJbpDDQwCuKGs5Zg2rcK7ZJauSUotTmWYQvNx+ZmWrUs5/j9Ee5FV2YonirGBQ9mc6u163kNlrIPFck062LGpahBhNmKDgod1o2PHTnRlZpEZNDIqU2D3hACgByxPjrY4vUnccV36ewLnQnYpp8szEu7PYTJr5dU5ltAekCAwEAAaNjMGEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAYYwHwYDVR0jBBgwFoAUaEEQwYKCQ1dm9+wLYBKRTlzxaDIwHQYDVR0OBBYEFGhBEMGCgkNXZvfsC2ASkU5c8WgyMA0GCSqGSIb3DQEBBAUAA4GBAHyhiv2CmH+vswkBjRA1Fzzk8ttu9s5kwqG0dXp25QRUWsGlr9nsKPNdVKt3P7p0A/KochHeeNiygiv+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,ENCRYPTEDDEK-Info: DES-EDE3-CBC,5053DC842B04612A1CnlF5Pqvd0zp2NLZ7iosxzTy6nDeXPpNyJpxB5q+V29IuY8Apb6TlJCU7YrsEB/nBTK7K76DCeGPlLpcuyEI171QmkQJ2gA0QhC0LrRo09WrINVH+b4So/y7nffZkVbp2yDpZwqoJ8cmRH94Tie0YmzBtEh6ayOud11z53qbrsCnfSEwszt1xrW1MKrFZrk/fTy6loHzGFzl3BDj4r5gBecExwcPp74ldHO+Ld4Nc9egG8BYkeBCsZZOQNVhXLNI0tODOs6hP915zb6OrZFYv0NK6grTBO9D8hjNZ3U79jJzsSP7UNzIYHNTzRJiAyui56Oy/iHvkCSNUIK6zeIJQnW4bSoM1BqrbVPwHU6QaXUqlNzZ8SDtw7ZRZ/rHuiDRTJMPbKquAzeuBss1132OaAUJRStjPXgyZTUbc+cWb6zATNws2yijPDTR6sRHoQL47wHMr2Yj80VZGgkCSLAkL88ACz9TfUiVFhtfl6xMC2yuFl+WRk1XfF5VtWe5Zer3Fn1DcBmlF7O86XUkiSHP4EV0cI6n5ZMzVLx0XAUtdAl1gD94y1V+6p9PcQHLyQApGRmj5IlSFw90aLafgCTbRbmC0ChIqHy91UFa1ub0130+yu7LsLGRlPmJ9NE61JRbjRhlUXItRYWY7C4M3m/0wz6fmVQNSumJM08RHq6lUB3olzIgGIZlZkoaESrLG0pqq2AENFemCPF0uhyVS2humMHjWuRr+jedfc/IMl7sLEgAdqCVCfV3RZVEaNXBud14QjkuTrwaTcRXVFbtrVioT/puyVUlpA7+k7w+F5TZwUV08mwvUEqDw==------END RSA PRIVATE KEY-----quit*!--- Copy and paste again the CERTIFICATE from the pem file, !--- followed by* **quit**. -----BEGIN CERTIFICATE-----
MIIB9zCCAWCgAwIBAgIBATANBgkqhkiG9w0BAQQFADAPMQ0wCwYDVQQDEwRteWNzMB4XDTA0MDkwMjIxMDI1NloXDTA3MDkwMjIxMDI1NlowDzENMAsGA1UEAxMEbXljczCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuGnnDXJbpDDQwCuKGs5Zg2rcK7ZJauSUotTmWYQvNx+ZmWrUs5/j9Ee5FV2YonirGBQ9mc6u163kNlrIPFck062LGpahBhNmKDgod1o2PHTnRlZpEZNDIqU2D3hACgByxPjrY4vUnccV36ewLnQnYpp8szEu7PYTJr5dU5ltAekCAwEAAaNjMGEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAYYwHwYDVR0jBBgwFoAUaEEQwYKCQ1dm9+wLYBKRTlzxaDIwHQYDVR0OBBYEFGhBEMGCgkNXZvfsC2ASkU5c8WgyMA0GCSqGSIb3DQEBBAUAA4GBAHyhiv2CmH+vswkBjRA1Fzzk8ttu9s5kwqG0dXp25QRUWsGlr9nsKPNdVKt3P7p0A/KochHeeNiygiv+hDQ3FVnzsNv983le6O5jvAPxc17RO1BbfNhqvEWMsXdnjHOcUy7XerCo+bdPcUf/eCiZueH/BEy/SZhD7yovzn2cdzBN-----END CERTIFICATE-----quit*!--- When you are prompted for the encryption key, !--- enter* **quit** to skip this step. quitRouter (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 del PKCS12**? Este ejemplo muestra que la restauración es de un archivo del PKCS12 y que la base de datos URL es NVRAM (el valor por defecto).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

Verificación

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

El comando show crypto pki server muestra la información sobre el servidor de la certificación.

```
Router#show crypto pki serverCertificate 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

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Soporte de productos de la Seguridad de routers
- Configuración y Administración de Cisco IOS Certificate Server para la Implementación de PKI
- Soporte Técnico y Documentación - Cisco Systems