Exemple de configuration de la sauvegarde et de la restauration d'un serveur d'autorité de certification IOS

Contenu

Introduction

Ce document décrit comment à de sauvegarde et à la restauration un serveur d'Autorité de certification (CA) de ® IOS pour le logiciel de Cisco IOS.

Référez-vous configurent et s'inscrivent un concentrateur de Cisco VPN 3000 à un routeur Cisco IOS comme un serveur CA afin de se renseigner plus sur la façon configurer un routeur Cisco IOS en tant que serveur CA.

Conditions préalables

Conditions requises

Prévoyez votre PKI avant que vous configuriez le serveur de certificat

Avant que vous configuriez Cisco IOS délivriez un certificat le serveur, il est important que vous ayez prévu pour et des valeurs appropriées choisies pour les configurations vous avez l'intention de utiliser dans votre PKI (tel que des vies de certificat et des vies de Liste des révocations de certificat (CRL)). Après que les configurations soient configurées dans le serveur de certificat et des Certificats sont accordés, des configurations ne peuvent pas être changées sans devoir modifier le serveur de certificat et re-s'inscrire les pairs. Pour les informations sur des valeurs par défaut et des configurations recommandées de serveur de certificat, référez-vous aux valeurs par défaut et aux valeurs recommandées de serveur de certificat.

Activez le serveur HTTP

Le serveur de certificat prend en charge l'inscription de certificat simple Protocol (SCEP) au-dessus du HTTP. Le serveur HTTP doit être activé sur le routeur pour que le serveur de certificat utilise SCEP. (Afin d'activer le serveur HTTP, utilisez la commande d'**ip http server**.) Le serveur de certificat active automatiquement ou des services des débronchements SCEP après le serveur HTTP sont activés ou désactivés. Si le serveur HTTP n'est pas activé, seulement l'inscription PKCS10 manuelle est prise en charge.

Services horaires dignes de confiance

Les Services horaires doivent s'exécuter sur le routeur parce que le serveur de certificat doit avoir la connaissance fiable de temps. Si une horloge de matériel est indisponible, le serveur de certificat dépend des configurations manuellement configurées d'horloge, telles que le Protocole NTP (Network Time Protocol). Référez-vous à la période de configuration et à la section de services de calendrier du guide de configuration de bases de configuration de Cisco IOS pour plus d'informations sur le NTP. S'il n'y a pas une horloge de matériel ou l'horloge est non valide, des affichages de ce message au démarrage :

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

Après que l'horloge soit réglée, le serveur de certificat commute automatiquement à l'état courant.

Composants utilisés

Les informations dans ce document sont basées sur le routeur de Cisco 3600 avec la version du logiciel Cisco IOS 12.4(8).

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Sauvegarde le serveur IOS CA

Àla configuration du serveur initiale de certificat, vous pouvez activer le certificat de CA et la clé CA à archiver automatiquement de sorte qu'ils puissent être restaurés plus tard si l'exemplaire original ou la configuration d'origine est perdu.

Quand le serveur de certificat est activé la première fois, le certificat de CA et la clé CA sont générés. Si des archives automatiques sont également activées, le certificat de CA et la clé CA est exporté (archivé) à la base de données du serveur. Les archives peuvent être dans PKCS12 ou format du Privacy Enhanced Mail (PEM).

Remarque:

- Ce fichier de sauvegarde de clé CA est extrêmement important et devrait être déplacé immédiatement à l'autre endroit sécurisé.
- Cette action de archivage se produit seulement une fois. Seulement la clé CA qui est manuellement générée et exportable marqué ou automatiquement générée par le serveur de certificat est archivée (cette clé est non-exportable marqué).
- Automatique-archivistique ne se produit pas si vous générez la clé CA manuellement et la marquez « non-exportable. »
- En plus du certificat de CA et du fichier d'archivage principal CA, vous devriez également régulièrement sauvegarder le fichier séquentiel (.ser) et le fichier CRL (.crl). Le fichier séquentiel et le fichier CRL sont les deux essentiels pour l'exécution CA si vous devez restaurer votre serveur de certificat.

Remarque: Il n'est pas possible de sauvegarder manuellement un serveur qui les clés RSA non-exportables d'utilisations ou les clés RSA non-exportables manuellement générées. Bien que des clés RSA automatiquement générées soient marquées en tant que non-exportable, elles sont automatiquement archivées une fois.

Exemple :

- **Format PEM** — Créez le CA et la sauvegarde les fichiers de la mémoire vive non volatile (NVRAM) (au serveur TFTP dans ce cas) :

```
!--- 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
```

- **Format PKCS12** — Créez le CA et la sauvegarde les fichiers de NVRAM (au serveur TFTP dans ce cas).

```
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
```

Restaurez le serveur IOS CA

Afin de restaurer le serveur CA, vous devez restaurer les fichiers **.ser** et **.crl**, recréer le serveur, et importer les données du PEM classez (format PEM) ou le fichier p12 (format PKCS12).

Dans notre scénario de laboratoire, l'**aucune** commande du **crypto pki server CA** n'est utilisée de retirer la configuration du serveur de certificat du routeur.

Exemple :

- **Format PEM** — Te permet pour visualiser le fichier PEM de sorte que vous puissiez copier et coller le certificat et l'introduire plus tard utilisant **plus de commande CA.pem**.Cet exemple prouve que la restauration est des archives PEM et que le database url est 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
```

- **Format PKCS12** — Cet exemple prouve que la restauration est des archives PKCS12 et que le database url est NVRAM (le par défaut).

```
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
```

Vérifiez

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

La commande de **show crypto pki server** affiche des informations sur le serveur de certification.

```
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
```

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Support produit de Sécurité des routeurs
- Configurant et gérant un serveur de certificat de Cisco IOS pour le déploiement de PKI
- Support et documentation techniques - Cisco Systems