# 备份与恢复IOS CA服务器配置示例

## 目录



## 简介

本文描述如何备份与恢复Cisco IOS软件的一个IOS® Certificate Authority (CA)服务器。

参考配置并且登记Cisco VPN 3000集中器到Cisco IOS路由器， CA服务器为了得知更多如何配置Cisco IOS路由器作为CA服务器。

## 先决条件

### 要求

**在您配置证书服务器前，请计划您的PKI**

在您配置Cisco IOS证书服务器前，它是您打算在您的PKI内使用的设置的重要您计划了为和选择的适当的值(例如证书寿命和证书撤销列表(CRL)寿命)。在设置在证书服务器后配置，并且证书授权，设置不可能更改，而不必重新配置证书服务器和再登记对等体。关于证书服务器默认设置和推荐的设置的信息，参考证书服务器默认值和推荐值。

**启用 HTTP 服务器**

证书服务器支持在HTTP的简单认证登记协议(SCEP)。在证书服务器的路由器必须启用HTTP服务器能使用SCEP。(为了启用HTTP服务器，请使用**ip http server命令**。)证书服务器自动地启用或功能失效在HTTP服务器以后的SCEP服务是启用或禁用的。如果HTTP服务器没有启用，只有支持手工的PKCS10登记。

**可靠时间服务**

因为证书服务器必须有可靠时间知识，时间服务一定运作在路由器。如果硬件时钟不可用，证书服

务器手工取决于配置的时钟设置，例如网络时间协议(NTP)。参考设置时间并且排进日程Cisco IOS配置基本原则配置指南的服务部分关于NTP的更多信息。如果没有硬件时钟或时钟无效，在启动的此信息显示：

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

在时钟设置后，对运行状态的自动证书服务器交换机。

## 使用的组件

本文档中的信息根据Cisco 3600路由器用Cisco IOS软件版本12.4(8)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

# 配置

本部分提供有关如何配置本文档所述功能的信息。

**注意：** 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

## 备份IOS CA服务器

在最初的证书服务器设置，您能启用自动地归档的CA证书和CA密钥，以便他们可以恢复的以后，如果原始复制或原始配置丢失。

当证书服务器第一次时启动， CA证书和CA密钥生成。如果自动存档也启用， CA证书和CA密钥导出(归档)对服务器数据库。存档可以在PKCS12或加强保密文件(PEM)格式。

**注意：**

- 此CA密钥备份文件是非常重要的，并且应该立即搬到另一个被巩固的地方。
- 此存档操作只发生一次。由证书服务器手工生成和被标记的可导出或自动地生成归档仅的CA密钥(此密钥是被标记的non-exportable)。
- 自动存档不发生，如果手工生成CA密钥并且标记它“non-exportable”。
- 除CA证书和CA归档文件之外，您应该有规律也备份序列文件(.ser)和CRL文件(.crl)。如果需要恢复您的证书服务器，序列文件和CRL文件CA操作的是两关键。

**注意：** 手工备份使用non-exportable RSA密钥或手工生成的non-exportable RSA密钥的服务器是不可能的。虽然自动地生成的RSA密钥被标记作为non-exportable，一次自动地归档他们。

**示例：**

- **PEM格式**—创建CA并且备份从非易失性RAM的文件(对TFTP server在这种情况下）：

```
!--- 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
```

- PKCS12格式—创建CA并且备份从NVRAM的文件(对TFTP server在这种情况下)。

```
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
```

## 恢复IOS CA服务器

为了恢复CA服务器，您需要恢复.ser和.crl文件，再创服务器和导入数据从PEM文件(PEM格式)或p12文件(PKCS12格式)。

在我们的实验室情形中， **crypto pki server CA**命令没有用于从路由器删除证书服务器配置。

**示例：**

- **PEM格式**—允许您查看PEM文件使用**更多CA.pem命令**，以便您能复制和插入证书和锁上以后。此示例显示恢复是从PEM存档，并且database url是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
```

- **PKCS12格式**—此示例显示恢复是从PKCS12存档，并且database url是NVRAM (默认)。

```
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
```

# 验证

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

**show crypto pki server命令**显示关于证明服务器的信息。

```
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
```

# 故障排除

目前没有针对此配置的故障排除信息。

# 相关信息

- 路由器安全产品支持
- 配置和管理PKI部署的一个Cisco IOS证书服务器
- 技术支持和文档 - Cisco Systems