IOS PKI自动注册、自动滚动更新和计时器

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[术语](#)
[配置](#)
[Cisco IOS CA服务器配置](#)
[客户端/分支路由器配置](#)
[自动注册操作](#)
[自动回滚正在运行](#)
[在Cisco IOS CA服务器上](#)
[在客户端路由器](#)
[PKI时间表示例，包括滚动和注册](#)
[重要注意事项](#)
[相关信息](#)

简介

本文档介绍自动注册和自动滚动更新的Cisco IOS®公钥基础设施(PKI)操作的工作方式，以及如何为这些操作计算各自的PKI计时器。

证书具有固定的生存期，并在某个时点过期。如果证书用于VPN解决方案的身份验证（例如），则这些证书的过期会导致可能的身份验证失败，从而导致终端之间的VPN连接丢失。为避免此问题，以下两种机制可用于自动证书续订：

- 客户端/分支路由器的自动注册
- 证书颁发机构(CA)服务器路由器的自动滚动

先决条件

要求

Cisco 建议您了解以下主题：

- PKI与信任概念
- 路由器上CA的基本配置

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息在特定实验室环境设备上创建。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。

术语

自动注册

当终端设备上的证书即将过期时，自动注册将获得新证书而不会中断。配置自动注册后，客户端/分支路由器可以在其自己的证书（称为其身份或ID证书）过期之前的某个时间请求新证书。

自动滚动

此参数决定证书服务器(CS)何时生成其滚动（阴影）证书；如果在CS配置下输入该命令而不使用任何参数，则默认时间为30天。

> **注意：**对于本文档中的示例，此参数的值为*10分钟*。

当CA服务器上的证书即将过期时，自动滚动使CA能够在不中断的情况下获得新证书。当配置了自动回滚时，CA路由器可以在其自己的证书过期之前的某个时间生成新证书。新证书(称为*影子*或*滚动*证书)在当前CA证书到期的精确时刻变为活动状态。

使用本文档介绍部分中提到的两项功能，PKI部署将变为自动化，并允许分支或客户端设备在当前CA证书到期之前获得卷影/滚动身份证书和卷影/滚动CA证书。这样，当其当前ID和CA证书到期时，它可以不中断地转换到新ID和CA证书。

lifetime ca-certificate

此参数指定CA证书的生存期。此参数的值可以以天/小时/分钟为单位指定。

> **注**意：对于本文档中的示例，此参数的值为*30分钟*。

有效期证书

此参数指定CA路由器颁发的身份证书的有效期。此参数的值可以以天/小时/分钟为单位指定。

> **注**意：对于本文档中的示例，此参数的值为*20分钟*

配置

> 注意:本文档中使用*lifetime*、*auto-rollover*和*auto-enroll*的较小PKI计时器值，以说明密钥自动注册和自动回滚的概念。在实时网络环境中，思科建议您使用这些参数的默认生存期。

> **提示**：如果没有权威时间源，则所有基于PKI计时器的事件(例如*滚动更新*和*重新注*册)都可能受到影响。因此，思科建议您在执行PKI的所有路由器上配置网络时间协议(NTP)。

Cisco IOS CA服务器配置

本节提供Cisco IOS CA服务器的配置示例。

```
RootCA#show ip interface brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 10.1.1.1 YES manual up up

crypto pki server ios-ca
issuer-name CN=Root-CA,OU=TAC,C=IN
grant auto
hash sha512
lifetime certificate 0 0 20
lifetime ca-certificate 0 0 30
cdp-url http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
auto-rollover 0 0 10
database url flash:
```

> **注**: 使用**auto-rollover 命令指定的值是当前CA证书生成之前的天数/小时数/分钟数。**因此，如果CA证书的有效期为12:00到12:30，则**auto-rollover 0 0 10**表示将在12:20左右生成全反CA证书。

输入**show crypto pki certificate**命令以验证Cisco IOS CA服务器上的配置：

```
RootCA#show crypto pki certificate
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: ios-ca
```

根据此输出，路由器包含有效期为2012年11月25日9:16至9:46的CA证书。由于自动回滚配置为10分钟，因此阴影/全反证书应由2012年11月*25日9.36* IST生成。

要确认，请输入**show crypto pki timer**命令：

```
RootCA#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:19:22.283 IST Sun Nov 25 2012
PKI Timers
| 12:50.930
| 12:50.930 SESSION CLEANUP
CS Timers
| 16:43.558
| 16:43.558  CS SHADOW CERT GENERATION
| 26:43.532 CS CERT EXPIRE
| 26:43.558 CS CRL UPDATE
```

根据此输出，在9.19 IST下发了**show crypto pki timer**命令，预计在16.43分钟内生成影子/全反证书

：

[09:19:22 + 00:16:43] = **09:36:05**，即[end-date_of_current_CA_cert - auto_rollover_timer];即[09:46:05 - 00:10:00] = **09:36:05**。

客户端/分支路由器配置

本节提供客户端/分支路由器的配置示例。

```
Client-1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 172.16.1.1 YES manual up up

crypto pki trustpoint client1
enrollment url http://10.1.1.1:80
subject-name CN=Client-1,OU=TAC,c=IN
revocation-check crl
auto-enroll 70 regenerate
```

> **注意**：**auto-enroll**命令在路由器上启用自动注册功能。命令语法为： **auto-enroll** [val %] [regenerate]。

在上一输出中，自动注册功能指定为70%;即，在[current_ID_cert的**生存期]的70%**时，路由器自动向CA重新注册。

> 提示: Cisco建议您将自动注册值设置为60%或更高，以确保PKI计时器正常工作。

*regenerate*选项导致为证书重新注册/续约目的创建新的Rivest-Shamir-Addleman(RSA)密钥。如果未指定此选项，则使用当前RSA密钥。

自动注册操作

要验证自动注册功能，请完成以下步骤：

1. 输入**crypto pki authenticate**命令以手动验证客户端路由器上的信任点：

   ```
   Client-1(config)#crypto pki authenticate client1
   ```

   注意：有关此命令的详细信息，请参阅《Cisco IOS安全命令参考》。
   输入命令后，应会显示类似以下的输出：

   ```
   Certificate has the following attributes:
   Fingerprint MD5: 006B2E44 37FBC3F1 AA14F32B CDC4462E
   Fingerprint SHA1: 2999CC53 8BF65247 C0D704E9 FDC73002 A33910D4

   % Do you accept this certificate? [yes/no]:
   ```
2. 键入**yes**以接受客户端路由器上的CA证书。然后，路**由**器上开始RENEW计时器：

```
Client-1#show crypto pki timer
PKI Timers
| 0.086
| 0.086 RENEW cvo-pki
| 9:51.366 SESSION CLEANUP
```

3. RENEW计**时器**达到零后，客户端路由器会自动向CA注册以获取其身份证书。收到证书后，输入**show crypto pki certificate**命令以查看该证书：

```
Client-1#show crypto pki certificate
Certificate
Status: Available
Certificate Serial Number (hex): 02
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:16:57 IST Nov 25 2012
end date: 09:36:57 IST Nov 25 2012
renew date: 09:30:08 IST Nov 25 2012
Associated Trustpoints: client1
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

续约日期为09:30:08，计算如下所示：

start-time +(%renewal of ID_cert_lifetime)

或者

09:16:57 +（70% * 20分钟）= **09:30:08**

PKI计时器反映的相同：

```
Client-1#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:19:01.714 IST Sun Nov 25 2012
PKI Timers
| 1:21.790
| 1:21.790 SESSION CLEANUP
| 11:06.894  RENEW client1
```

4. RENEW计时器过期后，路由器向CA重新注册以获取新的ID证书。在证书续订后，输入**show crypto pki cert**命令以查看新ID证书：

```
Client-1#show crypto pki cert
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:55.063 IST Sun Nov 25 2012
Certificate
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

请注意，不再有续*约日期*;相反，SHADOW计时器开始：

```
Client-1#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:57.922IST Sun Nov 25 2012
PKI Timers
```

```
| 25.582
| 25.582 SESSION CLEANUP
| 6:20.618 SHADOW client1
```

流程逻辑如下：

- 如果ID证书的结束日期不等于CA证书的结束日期，则根据自动注册百分比计算续约日期并启动RENEW计时器。
- 如果ID证书的结束日期等于CA证书的结束日期，则无需续约流程，因为当前ID证书仅在当前CA证书有效时才有效。相反，会启动SHADOW计时器。

此计时器也根据auto-enroll命令中提及的百分比计算。例如，考虑上例中显示的续约ID证书的有效日期：

```
Validity Date of current ID cert:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
```

此证书的有效期为16分钟。因此，滚动更新计时器（即SHADOW计时器）是16分钟的70%，大约等于11分钟。此计算意味着路由器开始请求其卷影/卷影证书，其地址为[09:30:09 + 00:11:00] = 09:41:09，与本文档前面所示的PKI SHADOW计时器相对应：

```
Client-1#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:57.922 IST Sun Nov 25 2012
PKI Timers
| 25.582
| 25.582 SESSION CLEANUP
| 6:20.618  SHADOW client1
```

自动回滚正在运行

本节介绍实际操作中的自动滚动功能。

在Cisco IOS CA服务器上

当SHADOW计时器过期时，CA路由器上会显示全反证书：

```
RootCA#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:36:28.184 IST Sun Nov 25 2012
CA Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Root-CA
cn=Root-CA
ou=TAC
c=IN
```

```
Validity Date:
 start date: 09:46:05 IST Nov 25 2012
end   date: 10:16:05 IST Nov 25 2012
Associated Trustpoints: ios-ca
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: ios-ca
```

在客户端路由器

如本文档前面所述，自动注册功能在客户端路由器上启动了SHADOW计时器。当SHADOW计时器过期时，自动注册功能使路由器能够请求CA服务器提供全反*/影子CA证*书。收到后，它还会查询其*滚动/卷影ID*证书。因此，路由器有两对证书：一对是当前的，另一对是包含全反/阴影证书：

```
Client-1#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:41:42.983 IST Sun Nov 25 2012
Router Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 05
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 09:50:09 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Root-CA
cn=Root-CA
```

```
ou=TAC
c=IN
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 10:16:05 IST Nov 25 2012
Associated Trustpoints: client1

Certificate
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

注意滚动更新ID证书的有效性：

```
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 09:50:09 IST Nov 25 2012
```

证书有效期仅为4分钟（而不是Cisco IOS CA服务器上配置的预期20分钟）。 根据Cisco IOS CA服务器，*绝对*ID证书生存期应为20分钟(这意味着，对于给定客户端路由器，向其颁发的ID证书（当前+阴影）的生存期总和不得超过20分钟)。

此过程在以下位置进一步描述：

- 以下是路由器上当前ID证书的有效性：

```
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
```

因此，*current_id_cert_lifetime*为16分钟。

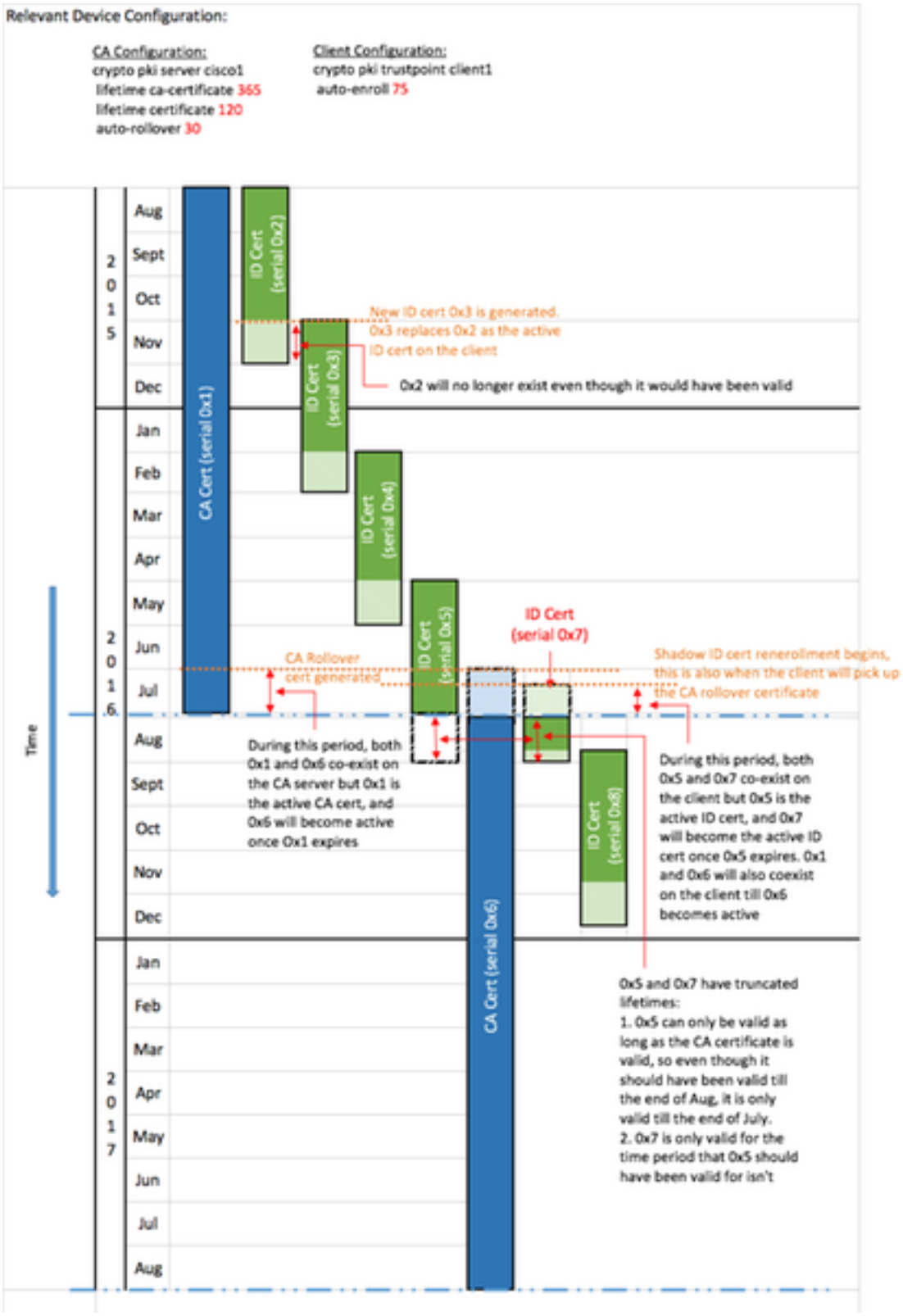
- 以下是滚动更新ID证书的有效性：

```
start date: 09:46:05 IST Nov 25 2012
end date: 09:50:09 IST Nov 25 2012
```

因此，*rollover_id_cert_lifetime*为四分钟。

- 根据Cisco IOS，当[current_id_cert_lifetime]添加到[rollover_id_cert_lifetime]时，它必须等于[total_id_cert_lifetime]。在本例中是这样。

PKI时间表示例，包括滚动和注册



重要注意事项

- PKI计时器需要授权时钟才能正常运行。思科建议您使用NTP来同步客户端路由器和Cisco IOS CA路由器之间的时钟。在没有NTP的情况下，可以使用路由器上的系统/硬件时钟。有关如何配置硬件时钟并使其具有权威性的信息，请参阅Cisco IOS版本12.4T的基本系统管理配置指南。

- 路由器重新加载时，NTP的同步通常需要几分钟。但是，PKI计时器几乎立即建立。自版本15.2(3.8)T和15.2(4)S起，NTP同步后会自动重新评估PKI计时器。

- PKI计时器不是绝对的；它们基于剩余*时间*，因此在重新启动后重新计算。例如，假设客户端路由器的ID证书有效期为100天，自动注册功能设置为80%。那么，预计在八十天后再注册。如果路由器在第60天重新加载，它将启动并重新计算PKI计时器，如下所示： (*剩余时*间)*(*%auto-enroll*)=(100-60)* 80% = 32天。

  因此，在[60 + 32] = 92天进行重新注册。

- 配置自动注册和自动回滚计时器时，必须使用允许PKI服务器上SHADOW CA证书可用性的值来配置它们，当PKI客户端请求时。这有助于缓解大规模环境中的潜在PKI服务故障。

相关信息

- **使用公钥基础设施部署Cisco IOS安全白皮书**
- **公用密钥基础结构:部署优势和功能白皮书**
- **公钥基础设施配置指南**
- **技术支持和文档 - Cisco Systems**