IOS PKI自動註冊、自動滾動和計時器

目錄

簡介

本文檔介紹自動註冊和自動滾動工作的Cisco IOS® Public Key Infrastructure(PKI)操作，以及如何為這些操作計算各自的PKI計時器。

證書具有固定的有效期並在某個點過期。如果證書用於VPN解決方案的身份驗證目的（例如），這些證書過期會導致可能的身份驗證失敗，從而導致終端之間的VPN連線丟失。為了避免此問題，可使用以下兩種機制自動續訂憑證：

- 客戶端/分支路由器的自動註冊
- 證書頒發機構(CA)伺服器路由器的自動滾動更新

必要條件

需求

思科建議您瞭解以下主題：

- PKI與信任概念
- 路由器上CA的基本配置

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

技術

自動註冊

當終端裝置上的證書即將到期時，自動註冊可獲取新證書而不會中斷。配置自動註冊後，客戶端/分支路由器可以在自己的證書（稱為其身份或ID證書）到期之前某個時間請求新證書。

自動回滾

此引數決定證書伺服器(CS)何時生成其翻轉（陰影）證書；如果在CS配置下輸入命令時沒有任何引數，則預設時間為30天。

> **附註**：對於本文檔中的示例，此引數的值為*10分鐘*。

當CA伺服器上的證書即將到期時，自動滾動更新可使CA獲取新證書而不會中斷。配置自動滾動更新時，CA路由器可以在其自己的證書到期之前生成新證書。新證書(稱為*shadow* 或*rolver*證書)將在當前CA證書到期時啟用。

通過使用本文檔的簡介部分中提到的兩項功能，PKI部署變為自動部署，並允許分支或客戶端裝置在當前CA證書到期之前獲取陰影/滾動身份證書和陰影/滾動更新CA證書。這樣，當新的ID和CA證書到期時，它就可以不間斷地過渡到新的ID和CA證書。

lifetime ca-certificate

此引數指定CA證書的生存期。此引數的值可以按天/小時/分鐘指定。

> **註**:對於本文檔中的示例，此引數的值為*30分鐘*。

生存期證書

此引數指定CA路由器頒發的身份證書的生存期。此引數的值可以按天/小時/分鐘指定。

> **註**:對於本文檔中的示例，此引數的值為*20分鐘*

設定

> **注意：本文檔中使用較小的用於*lifetime*、*auto-rollover*和*auto-enroll*的PKI計時器值，以說明金鑰自動註冊和自動翻轉概念。**在即時網路環境中，思科建議您使用這些引數的預設生存期。

> **提示**：如果沒有授權的時間源，則所有基於PKI計時器的事件(如*滾動更新*和**重新註冊)都會受到影響。**因此，思科建議您在執行PKI的所有路由器上配置網路時間協定(NTP)。

Cisco IOS CA伺服器配置

本節提供Cisco IOS CA伺服器的配置示例。

```
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:
```

> **註**:使用**auto-rollover命令指定的值是生成滾動更新證書的當前CA證書的結束日期之前的天數/小時/分鐘**。因此，如果CA證書的有效期是從12:00到12:30，則**auto-rollover 0 0 10**意味著在12:20左右生成滾動更新CA證書。

輸入**show crypto pki certificate**命令以驗證Cisco IOS CA伺服器上的配置：

```
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
```

根據此輸出，路由器包括有效期為2012年11月25日9:16至9:46的CA證書。由於自動滾動更新配置為10分鐘，因此預計在2012年11月25日*9.36IST之前生成陰影/*滾動更新證書。

若要確認，請輸入**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
```

基於此輸出，**show crypto pki timer**命令在9.19 IST發出，並且陰影/滾動更新證書預計在16.43分鐘

內生成：

[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**。

客戶端/分支路由器配置

本節提供客戶端/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
```

> **註**: **auto-enroll**命令在路由器上啟用自動註冊功能。命令語法為： **auto-enroll** [*val%*] [*regenerate*]。

在上一個輸出中，自動註冊功能被指定為70%;也就是說，在**[lifetime of current_ID_cert]**的70%處，路由器會自動向CA重新註冊。

> **提示**:思科建議您將auto-enroll值設定為60%或以上，以確保PKI計時器正常工作。

*regenerate*選項用於建立新的Rivest-Shamir-Addleman(RSA)金鑰，用於證書重新註冊/續訂。如果未指定此選項，則使用當前的RSA金鑰。

自動註冊操作

完成以下步驟以驗證自動註冊功能：

1. 輸入**crypto pki authenticate**命令以手動驗證客戶端路由器上的信任點：

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

   附註：有關此命令的詳細資訊，請參閱Cisco IOS安全命令參考。
   輸入命令後，系統會顯示類似以下的輸出：

   ```
   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. 輸入**yes**以接受客戶端路由器上的CA證書。接著，路由器上會開始**RENEW**計時器：

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

3. RENEW計時器達到零後，使用者端路由器會自動向CA註冊以取得其身分憑證。收到憑證後，輸入show crypto pki certificate命令以檢視：

```
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
```

續訂日期為09:30:08，計算方法如下所示：

開始時間+（%ID_cert_lifetime的續訂）

或

09:16:57 +（70% * 20分鐘）= 09:30:08

PKI計時器反映的情況相同：

```
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計時器到期後，路由器會向CA重新註冊以取得新的ID憑證。憑證續訂後，輸入show crypto pki cert命令以檢視新的ID憑證：

```
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
```

請注意，不再有續*訂日期*;相反，SHADOW計時器會開始：

```
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
```

以下是流程邏輯：

- 如果ID憑證的結束日期**不等於**CA憑證的結束日期，則根據自動註冊百分比計算續訂日期並啟動RENEW計時器。
- 如果**ID certificate 的結束日期等於CA證書的結束日期，則無需續訂過程，因為只有當前CA證書有效時，當前ID證書才有效。**而是啟動SHADOW計時器。

此計時器也根據**auto-enroll**命令中提到的百分比進行計算。例如，考慮上一示例中顯示的續訂ID證書的有效日期：

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

此證書的生存時間為16分鐘。因此，滾動更新計時器（即SHADOW計時器）是16分鐘的70%，約等於11分鐘。此計算意味著路由器在[09:30:09 + 00:11:00] = 09:41:09開始請求其影子/全反證書，該請求對應於本文檔前面顯示的PKI SHADOW計時器：

```
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
```

自動翻轉正在進行

本節介紹正在使用的自動翻轉功能。

在Cisco IOS CA伺服器上

SHADOW計時器到期時，CA路由器上會顯示滾動更新證書：

```
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
```

在客戶端路由器上

如本文檔前面所述，自動註冊功能在客戶端路由器上啟動SHADOW計時器。當SHADOW計時器到期時，自動註冊功能使路由器能夠請求CA伺服器獲取滾*動/陰影CA*證書。收到該證書後，它也會查詢*其翻轉/陰影ID*證書。因此，路由器有兩對憑證：一對是當前的，另一對包含全反/卷影證書：

```
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
```

請注意，滾動更新ID證書的有效性：

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

憑證有效期只有四分鐘（而不是Cisco IOS CA伺服器上設定的20分鐘）。 每個Cisco IOS CA伺服器的*絕對ID憑證存留時間應該為20分鐘(這表示對於指定的使用者端路由器，發給它的ID憑證（目前+陰影）的存留時間總和不得超過20分鐘)。*

以下將進一步介紹此過程：

- 以下是路由器上目前ID憑證的有效性：

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

因此，*current_id_cert_lifetime*為16分鐘。

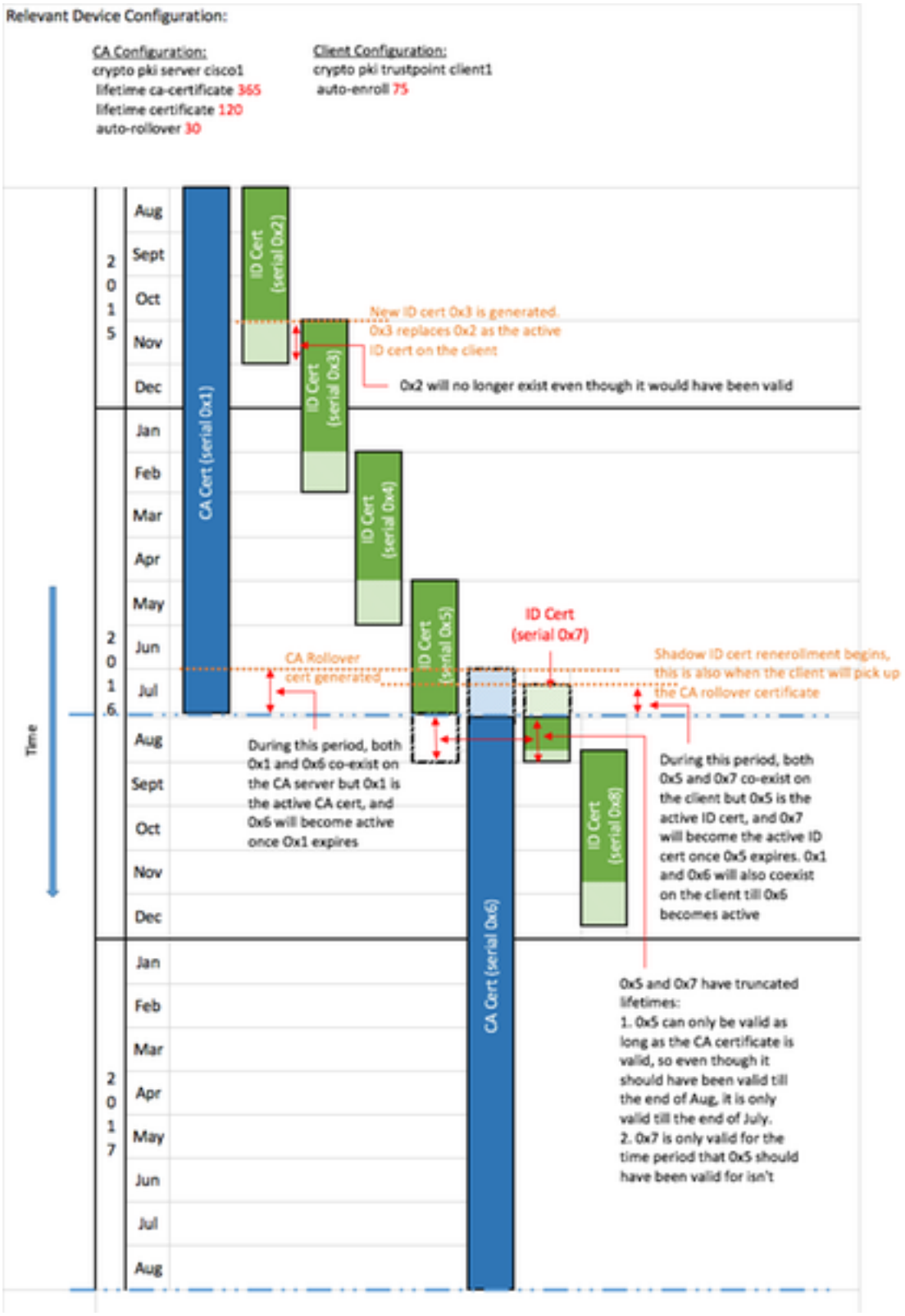
- 以下是滾動更新ID證書的有效性：

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

因此，*rollover_id_cert_lifetime*為四分鐘。

- 根據Cisco IOS，將[current_id_cert_lifetime]新增到[rollover_id_cert_lifetime]時，它必須等於[total_id_cert_lifetime]。這種情況屬實。

具有翻轉和註冊的PKI時間軸示例



重要注意事項

- PKI計時器需要授權時鐘才能正常工作。Cisco建議您使用NTP來同步客戶端路由器和Cisco IOS CA路由器之間的時鐘。如果沒有NTP，可以使用路由器上的系統/硬體時鐘。有關如何配置硬體時鐘並使其授權的資訊，請參閱基本系統管理配置指南(Cisco IOS版本12.4T)。

- 重新載入路由器時，NTP的同步通常需要幾分鐘。但是，PKI計時器幾乎立即建立。自15.2(3.8)T和15.2(4)S版本起，在NTP同步之後自動重新評估PKI計時器。

- PKI計時器不是絕對的；它們基於剩餘時*間*，因此會在重新引導後重新計算。例如，假設客戶端路由器的ID證書有效期為100天，且自動註冊功能設定為80%。然後，預計在第80天之後重新註冊。如果路由器在第60天重新載入，它將啟動並重新計算PKI計時器，如下所示：（*剩餘時間*）*（*%auto-enroll*）=（100-60）* 80% = 32天。

  因此，重新註冊發生於[60 + 32] = 92天。

- 配置自動註冊和自動註冊計時器時，務必在PKI客戶端請求證書時，在PKI伺服器上配置允許SHADOW CA證書可用性的值。這有助於緩解大規模環境中潛在的PKI服務故障。

相關資訊

- 使用公鑰基礎設施部署Cisco IOS安全白皮書
- Public Key Infrastructure:部署優勢和功能白皮書
- Public Key Infrastructure組態設定指南
- 技術支援與文件 - Cisco Systems