IOS PKI Auto-Enroll, Auto-Rollover e Timer

Sommario

Introduzione

In questo documento viene descritto come eseguire le operazioni di registrazione automatica e rollover automatico dell'infrastruttura a chiave pubblica (PKI) Cisco IOS® e come calcolare i rispettivi timer PKI per queste operazioni.

I certificati hanno una durata fissa e scadono a un certo punto. Se i certificati vengono utilizzati a scopo di autenticazione per una soluzione VPN (ad esempio), la scadenza di tali certificati può causare errori di autenticazione che comportano la perdita della connettività VPN tra gli endpoint. Per evitare questo problema, sono disponibili due meccanismi per il rinnovo automatico dei certificati:

- Registrazione automatica per router client/spoke
- Rollover automatico per il router server Autorità di certificazione (CA)

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- PKI e il concetto di fiducia
- Configurazione di base della CA sui router

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Terminologia

iscrizione automatica

Quando un certificato su un dispositivo terminale sta per scadere, la registrazione automatica ottiene un nuovo certificato senza interruzioni. Quando è configurata la registrazione automatica, il router client/spoke può richiedere un nuovo certificato prima della scadenza del proprio certificato (noto come certificato di identità o ID).

rollover automatico

Questo parametro decide quando il server certificati (CS) genera il proprio certificato di rollover (shadow); se il comando viene immesso nella configurazione CS senza alcun argomento, l'ora predefinita è 30 giorni.

> **Nota:** Per gli esempi di questo documento, il valore del parametro è *10 minuti*.

Quando un certificato sul server CA sta per scadere, il rollover automatico consente alla CA di ottenere un nuovo certificato senza interruzioni. Quando è configurato il rollover automatico, il router della CA può generare un nuovo certificato in un determinato momento prima della scadenza del proprio certificato. Il nuovo certificato, denominato certificato *shadow* o *rollover*, diventa attivo nel momento esatto in cui scade il certificato CA corrente.

Con l'utilizzo delle due funzionalità menzionate nella sezione Introduzione di questo documento, la distribuzione PKI diventa automatizzata e consente al dispositivo spoke o client di ottenere un certificato di identità shadow/rollover e un certificato CA shadow/rollover prima della scadenza del certificato CA corrente. In questo modo, può passare senza interruzioni ai nuovi certificati ID e CA quando scadono i certificati ID e CA correnti.

certificato ca

Questo parametro specifica la durata del certificato CA. Il valore di questo parametro può essere specificato in giorni/ore/minuti.

> **Nota**: per gli esempi riportati in questo documento, il valore di questo parametro è *30 minuti*.

certificato di durata

Questo parametro specifica la durata del certificato di identità rilasciato dal router CA. Il valore di questo parametro può essere specificato in giorni/ore/minuti.

> **Nota**: per gli esempi di questo documento, il valore del parametro è *20 minuti*

Configurazione

> **Nota**: in questo documento vengono utilizzati valori timer PKI più piccoli per *durata*, *rollover automatico* e *registrazione automatica* per illustrare i concetti chiave di registrazione automatica e rollover automatico. In un ambiente di rete attivo, Cisco consiglia di utilizzare le durate predefinite per questi parametri.

> **Suggerimento**: tutti gli eventi basati su timer PKI, ad esempio il *rollover* e la *registrazione*, possono essere influenzati se non esiste un'origine ora autorevole. Per questo motivo, Cisco consiglia di configurare Network Time Protocol (NTP) su tutti i router che eseguono PKI.

Configurazione server CA Cisco IOS

In questa sezione viene fornita una configurazione di esempio per il server CA Cisco IOS.

```
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:
```

> **Nota**: il valore specificato con il comando **auto-rollover** è il numero di giorni/ore/minuti *prima della data di fine del* certificato *CA corrente* generato dal certificato di rollover. Pertanto, se un certificato CA è valido dalle 12:00 alle 12:30, il **rollover automatico 0 0 10** implica che il certificato CA di rollover viene generato intorno alle 12:20.

Immettere il comando **show crypto pki certificate** per verificare la configurazione sul server CA Cisco IOS:

```
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
```

In base a questo output, il router include un certificato CA valido dal 25 novembre 2012 dalle 9:16 alle 9:46. Poiché il rollover automatico è configurato per 10 minuti, il certificato di shadow/rollover dovrebbe essere generato entro il *9.36 IST* Nov 25, 2012.

Per confermare, immettere il comando **show crypto pki timer**:

```
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
```

In base a questo output, il comando **show crypto pki timer** è stato emesso alle 9.19 IST e il certificato shadow/rollover dovrebbe essere generato entro 16.43 minuti:

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

Configurazione client/router spoke

In questa sezione viene fornita una configurazione di esempio per il router client/spoke.

```
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
```

> **Nota**: il comando **auto-enroll** abilita la funzionalità di registrazione automatica sul router. Sintassi del comando: **auto-enroll** [*val%*] [*regenerate*].

Nell'output precedente, la funzione di registrazione automatica è specificata come 70%; ovvero al 70% di **[lifetime of current_ID_cert]**, il router si riconnette automaticamente con la CA.

> **Suggerimento**: Cisco consiglia di impostare il valore di registrazione automatica su 60% o più per garantire il corretto funzionamento dei timer PKI.

L'opzione *regenerate* comporta la creazione di una nuova chiave RSA (Rivest-Shamir-Addleman) per il rinnovo e il rinnovo dei certificati. Se questa opzione non è specificata, viene utilizzata la chiave RSA corrente.

Iscrizione Automatica In Azione

Per verificare la funzionalità di iscrizione automatica, completare i seguenti passaggi:

1. Immettere il comando **crypto pki authentication** per autenticare manualmente il trust point sul router client:

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

   Nota: Per ulteriori informazioni sul comando, consultare la guida di riferimento dei comandi di Cisco IOS Security.
   Dopo aver immesso il comando, dovrebbe essere visualizzato un output simile al seguente:

   ```
   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. Digitare **yes** per accettare il certificato CA sul router client. Quindi, inizia un timer di **rinnovo** sul router:

   ```
   Client-1#show crypto pki timer
   PKI Timers
   | 0.086
   | 0.086 RENEW cvo-pki
   | 9:51.366 SESSION CLEANUP
   ```
3. Quando il timer di **rinnovo** raggiunge lo zero, il router client si registra automaticamente presso la CA per ottenere il proprio certificato di identità. Dopo aver ricevuto il certificato, immettere il comando **show crypto pki certificate** per visualizzarlo:

   ```
   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
```

La **data di rinnovo** è **09.30.08** ed è calcolata come illustrato di seguito:

ora di inizio + (%rinnovo di ID_cert_lifetime)

O

09:16:57 + (70% * 20 minuti) = **09:30:08**

I timer PKI riflettono la stessa situazione:

```
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. Dopo la scadenza del timer di **rinnovo**, il router si registra nuovamente presso la CA per ottenere un nuovo certificato ID. Dopo aver rinnovato il certificato, immettere il comando **show crypto pki cert** per visualizzare il nuovo certificato ID:

```
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
```

Si noti che non esiste più una *data di rinnovo*; viene invece avviato un timer **SHADOW**:

```
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
```

La logica del processo è la seguente:

- Se la data di fine del certificato ID **non è uguale** alla data di fine del certificato **CA**, calcolare una data di rinnovo in base alla percentuale di registrazione automatica e avviare il **timer RENEW**.
- Se la data di fine del certificato **ID è uguale** alla data di fine del certificato **CA**, non è necessario alcun processo di rinnovo poiché il certificato ID corrente è valido solo finché il certificato CA corrente è valido. Viene invece avviato un timer **SHADOW**.

Anche questo timer viene calcolato in base alla percentuale indicata nel comando **auto-enroll**. Si considerino, ad esempio, le date di validità del certificato ID rinnovato visualizzate nell'esempio precedente:

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

La durata del certificato è di 16 minuti. Pertanto, il timer di rollover (ovvero il timer SHADOW) è il 70% di 16 minuti, ovvero circa 11 minuti. Questo calcolo implica che il router inizia le richieste per i propri certificati shadow/rollover a [09:30:09 + 00:11:00] = 09:41:09, che corrisponde al timer SHADOW PKI mostrato in precedenza in questo documento:

```
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
```

Rollover automatico in azione

Questa sezione descrive la funzione di rollover automatico in azione.

Sul server CA Cisco IOS

Alla scadenza del timer SHADOW, il certificato di rollover viene visualizzato sul router CA:

```
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
```

Sul router client

Come descritto in precedenza in questo documento, la funzione di registrazione automatica ha avviato un timer SHADOW sul router client. Alla scadenza del timer SHADOW, la funzione di registrazione automatica consente al router di richiedere al server CA il certificato *CA di rollover/shadow*. Una volta ricevuto, richiede anche il certificato *ID rollover/shadow*. Di conseguenza, il router ha due coppie di certificati: una coppia corrente e l'altra coppia contenente i certificati rollover/shadow:

```
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
```

Notare la validità del certificato ID rollover:

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

La durata del certificato è di soli quattro minuti (anziché i 20 minuti previsti, come configurato sul server CA Cisco IOS). In base al server CA Cisco IOS, la durata *assoluta* del certificato ID deve essere di 20 minuti (ovvero, per un determinato router client, la somma della durata dei certificati ID (corrente + shadow) rilasciati non deve essere superiore a 20 minuti).

Questo processo è descritto più avanti:

- Di seguito è riportata la validità del certificato ID corrente sul router:

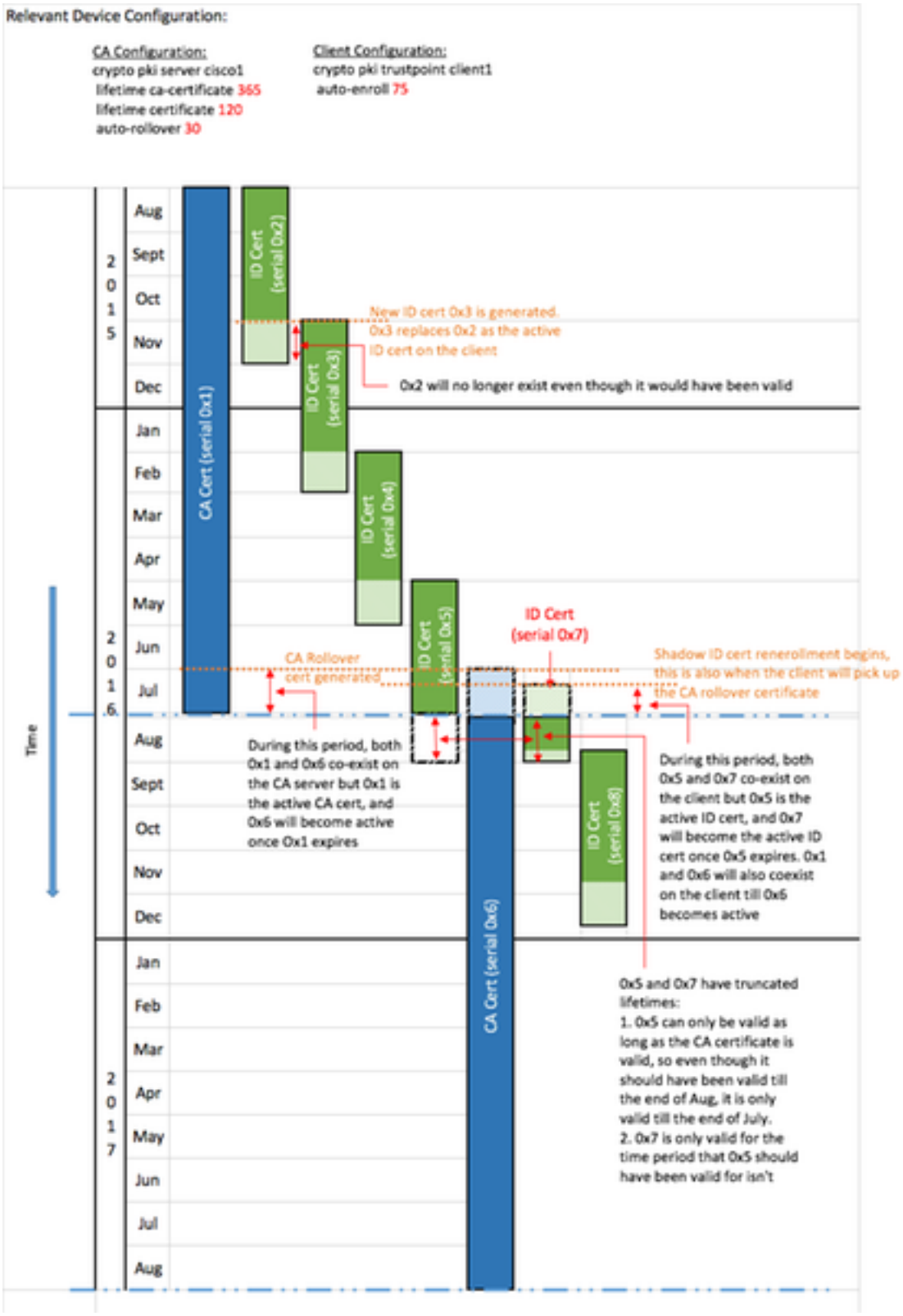
  ```
  start date: 09:30:09 IST Nov 25 2012
  end date: 09:46:05 IST Nov 25 2012
  ```

  Pertanto, il valore di *current_id_cert_lifetime* è 16 minuti.
- Di seguito è riportata la validità del certificato ID rollover:

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

  Pertanto, il valore di *rollover_id_cert_lifetime* è pari a quattro minuti.
- In base a Cisco IOS, quando [current_id_cert_lifetime] viene aggiunto a [rollover_id_cert_lifetime], deve essere uguale a [total_id_cert_lifetime]. Ciò è vero in questo caso.

Sequenza temporale PKI di esempio con rollover e registrazione



Considerazioni importanti

- Per funzionare correttamente, i timer PKI richiedono un orologio autorevole. Cisco consiglia di utilizzare il protocollo NTP per sincronizzare gli orologi tra i router client e il router CA Cisco IOS. In assenza di NTP, è possibile usare l'orologio di sistema/hardware del router. Per informazioni su come configurare l'orologio hardware e renderlo autorevole, fare riferimento alla guida alla configurazione di base della gestione del sistema, Cisco IOS versione 12.4T.

- Al riavvio di un router, la sincronizzazione dell'NTP spesso richiede qualche minuto. Tuttavia, i

timer PKI vengono stabiliti quasi immediatamente. A partire dalle versioni 15.2(3.8)T e 15.2(4)S, i timer PKI vengono automaticamente rivalutati dopo la sincronizzazione NTP.

- I timer PKI non sono assoluti; sono basati sul *tempo rimanente* e vengono quindi ricalcolati dopo un riavvio. Si supponga, ad esempio, che il router client disponga di un certificato ID valido per 100 giorni e che la funzione di registrazione automatica sia impostata sull'80%. In questo caso, la registrazione dovrebbe essere eseguita dopo l'ottantesimo giorno. Se il router viene ricaricato il 60° giorno, si avvia e ricalcola il timer PKI come mostrato di seguito: (*tempo rimanente*) * (*%registrazione automatica*) = (100-60) * 80% = 32 giorni.

  Pertanto, la registrazione viene eseguita il [60 + 32] = 92° giorno.

- Quando si configurano i timer di registrazione e di registrazione automatica, è importante configurarli con valori che consentano la disponibilità del certificato CA SHADOW nel server PKI quando il client PKI ne richiede uno. Ciò consente di ridurre i potenziali errori dei servizi PKI in un ambiente su larga scala.

Informazioni correlate

- White paper sull'implementazione della sicurezza Cisco IOS con un'infrastruttura a chiave pubblica
- Infrastruttura a chiave pubblica: White paper sui vantaggi e le caratteristiche dell'installazione
- Guida alla configurazione dell'infrastruttura a chiave pubblica
- Documentazione e supporto tecnico – Cisco Systems