IOS PKI Auto-Enroll, Auto-Rollover y Timers

Contenido

Introducción

Este documento describe cómo funcionan las operaciones de Cisco IOS® Public Key Infrastructure (PKI) de inscripción automática y renovación automática y cómo se calculan los temporizadores PKI respectivos para estas operaciones.

Los certificados tienen una duración fija y caducan en algún momento. Si los certificados se utilizan con fines de autenticación para una solución VPN (por ejemplo), la expiración de estos certificados conlleva posibles fallos de autenticación que resultan en la pérdida de conectividad VPN entre los terminales. Para evitar este problema, estos dos mecanismos están disponibles para la renovación automática del certificado:

- Inscripción automática para los routers cliente/spoke
- Renovación automática para el router de servidor de la Autoridad de certificación (CA)

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- PKI y el concepto de confianza
- Configuración básica de CA en routers

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información de este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Terminology

inscripción automática

Cuando un certificado de un dispositivo final está a punto de caducar, la inscripción automática obtiene un nuevo certificado sin interrupciones. Cuando se configura la inscripción automática, el router cliente/spoke puede solicitar un nuevo certificado en algún momento antes de que caduque su propio certificado (conocido como su certificado de identidad o ID).

auto-rollover

Este parámetro decide cuándo el servidor de certificados (CS) genera su certificado de renovación (sombra); si se ingresa el comando en la configuración CS sin ningún argumento, el tiempo predeterminado es 30 días.

> **Nota:** Para los ejemplos de este documento, el valor de este parámetro es *10 minutos*.

Cuando un certificado del servidor de la CA está a punto de caducar, la renovación automática permite a la CA obtener un nuevo certificado sin interrupciones. Cuando se configura la renovación automática, el router de la CA puede generar un nuevo certificado en algún momento antes de que su propio certificado caduque. El nuevo certificado, que se denomina el certificado *sombra* o *renovación*, se activa en el momento preciso en que caduca el certificado de CA actual.

Con el uso de las dos funciones que se mencionan en la sección Introducción de este documento, la implementación PKI se automatiza y permite que el dispositivo spoke o cliente obtenga un certificado de identidad Shadow/rollover y un certificado de CA Shadow/rollover antes del vencimiento del certificado de CA actual. De esta manera, puede realizar la transición sin interrupciones a los nuevos certificados de ID y CA cuando caduquen sus certificados de ID y CA actuales.

lifetime ca-certificate

Este parámetro especifica la duración del certificado de CA. El valor de este parámetro se puede especificar en días/horas/minutos.

> **Nota**: Para los ejemplos de este documento, el valor de este parámetro es *30 minutos*.

certificado de vida

Este parámetro especifica la duración del certificado de identidad emitido por el router CA. El valor de este parámetro se puede especificar en días/horas/minutos.

Nota: Para los ejemplos de este documento, el valor de este parámetro es *20 minutos*

Configurar

Nota: En este documento se utilizan valores de temporizador PKI menores para *vida útil*, *renovación automática* y *inscripción automática* **para ilustrar conceptos clave de inscripción automática y renovación automática.** En un entorno de red activo, Cisco recomienda utilizar los tiempos de vida predeterminados para estos parámetros.

Sugerencia: todos los eventos basados en temporizador PKI, como *rollover* y *reinscribirse*, pueden verse afectados si no hay un origen de tiempo autorizado. Por esta razón, Cisco recomienda que configure el protocolo de tiempo de red (NTP) en todos los routers que realizan PKI.

Configuración del servidor CA de Cisco IOS

Esta sección proporciona un ejemplo de configuración para el servidor CA de 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: El valor especificado con el comando **auto-rollover** es el número de días/horas/minutos *antes de la fecha de finalización del certificado de CA actual* **que se genera el certificado de renovación.** Por lo tanto, si un certificado de CA es válido de 12:00 a 12:30, **auto-rollover 0 0 10** implica que el certificado de CA de renovación se genera alrededor de 12:20.

Ingrese el comando **show crypto pki certificate** para verificar la configuración en el servidor CA de 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
```

Basándose en esta salida, el router incluye un certificado de CA válido de 9:16 a 9:46 IST el 25 de noviembre de 2012. Dado que la renovación automática se configura durante 10 minutos, se espera que el certificado de renovación/sombra se genere antes del *9.36 IST* el 25 de noviembre de 2012.

Para confirmar, ingrese el 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
```

En base a esta salida, el comando **show crypto pki timer** se emitió en IST 9.19, y se espera que el certificado de sombra/renovación se genere en 16.43 minutos:

[09:19:22 + 00:16:43] = **09:36:05**, que es el [end-date_of_current_CA_cert - auto_rollover_timer]; es decir, [09:46:05 - 00:10:00] = **09:36:05**.

Configuración del router de cliente/radio

Esta sección proporciona un ejemplo de configuración para el router cliente/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**: El comando **auto-enroll** habilita la función de inscripción automática en el router. La sintaxis del comando es: **auto-enroll** [*val%*] [*regenerate*].

En el resultado anterior, la función de inscripción automática se especifica como 70%; es decir, con el 70% de la **[vida útil de current_ID_cert]**, el router se vuelve a inscribir automáticamente con la CA.

Sugerencia: Cisco recomienda que establezca el valor de inscripción automática en un 60% o más para asegurarse de que los temporizadores PKI funcionen correctamente.

La opción *regenerar* lleva a la creación de una nueva clave Rivest-Shamir-Addleman (RSA) para fines de renovación/renovación de certificados. Si no se especifica esta opción, se utiliza la clave RSA actual.

Inscripción automática en acción

Complete estos pasos para verificar la función de inscripción automática:

1. Ingrese el comando **crypto pki authenticate** para autenticar manualmente el punto de confianza en el router cliente:

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

Nota: Para obtener más información sobre este comando, consulte la Referencia de Comandos de Seguridad de Cisco IOS.
Una vez que ingrese el comando, debería aparecer un resultado similar a este:

```
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. Escriba **yes** para aceptar el certificado de CA en el router cliente. Luego, un temporizador **RENEW** comienza en el router:

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

3. Una vez que el temporizador **RENEW** alcanza cero, el router cliente se inscribe automáticamente con la CA para obtener su certificado de identidad. Una vez recibido el certificado, ingrese el comando **show crypto pki certificate** para verlo:

```
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 **fecha de renovación** es **09:30:08** y se calcula como se muestra aquí:

tiempo de inicio + (%renovación de ID_cert_lifetime)

O bien

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

Los temporizadores PKI reflejan lo mismo:

```
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. Una vez que caduca el temporizador **RENEW**, el router se vuelve a inscribir en la CA para obtener un nuevo certificado de ID. Después de que se haya producido una renovación del certificado, ingrese el comando **show crypto pki cert** para ver el nuevo certificado de 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
```

Observe que ya no existe una *fecha de renovación*; en su lugar, comienza un temporizador **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
```

Esta es la lógica del proceso:

- Si la fecha de finalización del certificado de ID **no es igual** a la fecha de finalización del certificado de la **CA, calcule una fecha de renovación basándose en el porcentaje de inscripción automática e inicie el temporizador** RENEW.
- Si la fecha de finalización del **certificado de ID es igual** a la fecha de finalización del certificado de **CA**, no es necesario ningún proceso de renovación, ya que el certificado de ID actual es válido sólo mientras el certificado de CA actual sea válido. En su lugar, se inicia un temporizador **SHADOW**.

Este temporizador también se calcula en función del porcentaje mencionado en el comando **auto-enroll**. Por ejemplo, considere las fechas de validez del certificado de ID renovado que se muestran en el ejemplo anterior:

```
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 duración de este certificado es de 16 minutos. Por lo tanto, el temporizador de reversión (es decir, el temporizador SHADOW) es del 70% de 16 minutos, lo que equivale aproximadamente a 11 minutos. Este cálculo implica que el router comienza las solicitudes de sus certificados de sombra/renovación a las [09:30:09 + 00:11:00] = 09:41:09, que corresponde al temporizador PKI SHADOW que se muestra anteriormente en este 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
```

Renovación automática en acción

En esta sección se describe la función de renovación automática en acción.

En el servidor CA de Cisco IOS

Cuando caduca el temporizador SHADOW, aparece el certificado de renovación en el 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
```

En el router del cliente

Como se describió anteriormente en este documento, la función de inscripción automática inició un temporizador SHADOW en el router del cliente. Cuando caduca el temporizador SHADOW, la función de inscripción automática permite al router solicitar al servidor de la CA el certificado *de sustitución/sombra de CA*. Una vez recibida, consulta también su certificado *rollover/Shadow ID*. Como resultado, el router tiene dos pares de certificados: un par que es actual y el otro que contiene los certificados de renovación/sombra:

```
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
```

Observe la validez del certificado de ID de renovación:

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

La duración del certificado es de sólo cuatro minutos (en lugar de los 20 minutos esperados, como se configuró en el servidor de CA de Cisco IOS). Según el servidor de CA de Cisco IOS, la duración del certificado de ID *absoluta* debe ser de 20 minutos (lo que significa que, para un router cliente determinado, la suma de las duraciones de los certificados de ID (actual + sombra) emitidos no debe ser superior a 20 minutos).

Este proceso se describe a continuación:

- Esta es la validez del certificado de ID actual en el router:

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

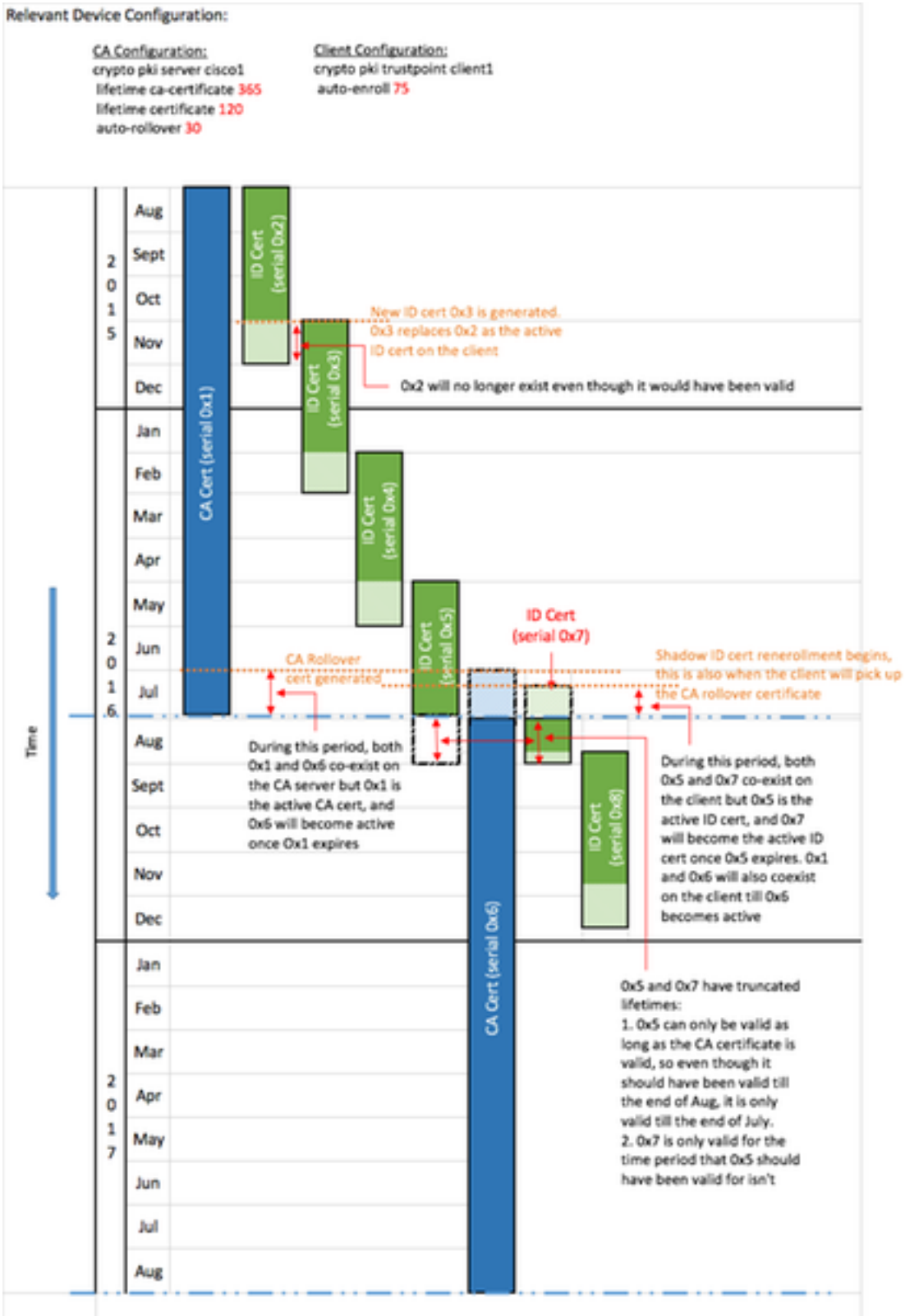
  Por lo tanto, el *current_id_cert_lifetime* es de 16 minutos.
- Esta es la validez del certificado de ID de renovación:

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

Por lo tanto, el *rollover_id_cert_lifetime* es de cuatro minutos.

- Según Cisco IOS, cuando se agrega [current_id_cert_lifetime] a [rollover_id_cert_lifetime], debe ser igual a [total_id_cert_lifetime]. Esto es cierto en este caso.

Línea de tiempo PKI de muestra con Rollover e Inscripción



Consideraciones importantes

- Los temporizadores PKI requieren un reloj autorizado para funcionar correctamente. Cisco recomienda que utilice NTP para sincronizar los relojes entre los routers cliente y el router CA de Cisco IOS. En ausencia de NTP, se puede utilizar el reloj del sistema/hardware del router. Para obtener información sobre cómo configurar el reloj de hardware y convertirlo en autoritativo, refiérase a la Guía de Configuración de Administración Básica del Sistema, Cisco IOS Release 12.4T.

- Tras la recarga de un router, la sincronización del NTP a menudo toma unos minutos. Sin embargo, los temporizadores PKI se establecen casi inmediatamente. A partir de las versiones 15.2(3.8)T y 15.2(4)S, los temporizadores PKI se reevalúan automáticamente después de que se sincronice el NTP.

- Los temporizadores PKI no son absolutos; se basan en el *tiempo restante* y, por lo tanto, se vuelven a calcular después de un reinicio. Por ejemplo, suponga que el router del cliente tiene un certificado de ID válido durante 100 días y que la función de inscripción automática está configurada en el 80%. Luego, se espera que la reinscripción ocurra después del día 80. Si el router se recarga en el día 60, se inicia y vuelve a calcular el temporizador PKI como se muestra aquí: (*tiempo restante*) * (*%auto-enroll*) = (100-60) * 80% = 32 días.

  Por lo tanto, la reinscripción se produce en el [60 + 32] = 92º día.

- Cuando configura los auto-enroll y auto-rollovertimers, es importante configurarlos con valores que permitan la disponibilidad del certificado SHADOW CA en el servidor PKI cuando el cliente PKI solicita uno. Esto ayuda a mitigar los posibles fallos de los servicios PKI en un entorno a gran escala.

Información Relacionada

- Informe técnico sobre la implementación de la seguridad de Cisco IOS con una infraestructura de clave pública
- Infraestructura de clave pública: Informe técnico sobre las características y ventajas de la implementación
- Guía de Configuración de Public Key Infrastructure
- Soporte Técnico y Documentación - Cisco Systems