Inscrição automática de PKI do IOS, rollover automático e temporizadores

Contents

Introduction

Este documento descreve como as operações de PKI (Public Key Infrastructure, Infraestrutura de Chave Pública) do Cisco IOS® de registro automático e rollover automático e como os respectivos temporizadores PKI são calculados para essas operações.

Os certificados têm vida útil fixa e expiram em algum momento. Se os certificados forem usados para fins de autenticação para uma solução VPN (por exemplo), a expiração desses certificados levará a possíveis falhas de autenticação que resultam na perda de conectividade VPN entre os pontos finais. Para evitar esse problema, esses dois mecanismos estão disponíveis para renovação automática de certificado:

- Inscrição automática para os roteadores cliente/spoke
- Rollover automático para o roteador de servidor da Autoridade de Certificação (CA)

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- PKI e o conceito de confiança
- Configuração básica de CA em roteadores

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações apresentadas neste documento foram criadas a partir de dispositivos em um ambiente de laboratório 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

inscrição automática

Quando um certificado em um dispositivo final está prestes a expirar, a inscrição automática obtém um novo certificado sem interrupção. Quando a inscrição automática é configurada, o roteador do cliente/spoke pode solicitar um novo certificado em algum momento antes que seu próprio certificado (conhecido como sua identidade ou certificado de ID) expire.

rollover automático

Este parâmetro decide quando o Servidor de Certificados (CS) gera seu certificado de sobreposição (sombra); se o comando for inserido na configuração do CS sem nenhum argumento, a hora padrão será 30 dias.

> **Note**: Para os exemplos neste documento, o valor deste parâmetro é *10 minutos*.

Quando um certificado no servidor CA está prestes a expirar, a transferência automática permite que a AC obtenha um novo certificado sem interrupção. Quando a transferência automática é configurada, o roteador CA pode gerar um novo certificado em algum momento antes que seu próprio certificado expire. O novo certificado, que é chamado de *sombra* ou *sobreposição* de certificado, torna-se ativo no momento exato em que o certificado CA atual expira.

Com o uso dos dois recursos mencionados na seção Introdução deste documento, a implantação de PKI se torna automatizada e permite que o dispositivo spoke ou cliente obtenha um certificado de identidade de sombra/rollover e um certificado de CA de sombra/rollover antes da expiração do certificado de CA atual. Dessa forma, ele pode fazer a transição sem interrupção para os novos certificados de ID e CA quando seus certificados de ID e CA atuais expirarem.

lifetime ca-certificate

Este parâmetro especifica o tempo de vida do certificado CA. O valor deste parâmetro pode ser especificado em dias/horas/minutos.

> **Observação**: para os exemplos neste documento, o valor deste parâmetro é *30 minutos*.

certificado vitalício

Esse parâmetro especifica o tempo de vida do certificado de identidade emitido pelo roteador CA. O valor deste parâmetro pode ser especificado em dias/horas/minutos.

Observação: para os exemplos neste documento, o valor deste parâmetro é *20 minutos*

Configurar

Nota: Valores de temporizador PKI menores para *vida útil*, *rollover automático* e *inscrição automática* são usados neste documento para ilustrar os conceitos chave de inscrição automática e de substituição automática. Em um ambiente de rede ativa, a Cisco recomenda que você use os tempos de vida padrão para esses parâmetros.

Dica: todos os eventos baseados em temporizador PKI, como *rollover* e *reinscrição*, podem ser afetados se não houver uma fonte de tempo autoritativa. Por esse motivo, a Cisco recomenda que você configure o Network Time Protocol (NTP) em todos os roteadores que executam PKI.

Configuração do servidor Cisco IOS CA

Esta seção fornece um exemplo de configuração para o servidor de CA do 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: O valor especificado com o comando **autorrollover** é o número de dias/horas/minutos *antes da data final do* certificado *CA atual* que o certificado de rollover é gerado. Portanto, se um certificado CA for válido das 12:00 às 12:30, a **rollover 0 0 10 automática** implica que o certificado CA de rollover é gerado em torno das 12:20.

Insira o comando **show crypto pki certificate** para verificar a configuração no servidor de CA do 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
```

Com base nessa saída, o roteador inclui um certificado CA válido de 9:16 a 9:46 IST de 25 de novembro de 2012. Como a rollover automática está configurada para 10 minutos, espera-se que o certificado de sombra/rollover seja gerado por *IST* de *9,36* de 25 de novembro de 2012.

Para confirmar, insira o 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
```

Com base nessa saída, o comando **show crypto pki timer** foi emitido em 9.19 IST, e espera-se que o certificado shadow/rollover seja gerado em 16,43 minutos:

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

Configuração do roteador do cliente/spoke

Esta seção fornece um exemplo de configuração para o roteador do 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
```

> **Observação**: o comando **autoenroll** ativa o recurso de inscrição automática no roteador. A sintaxe do comando é: **autoenroll** [*val%*] [*regenerate*].

Na saída anterior, o recurso de inscrição automática é especificado como 70%; ou seja, em 70% do **[duração do current_ID_cert]**, o roteador se registra automaticamente com a CA.

> **Dica**: a Cisco recomenda que você defina o valor da inscrição automática como 60% ou mais para garantir que os temporizadores PKI funcionem corretamente.

A opção *regenerar* leva à criação de uma nova chave Rivest-Shamir-Addleman (RSA) para fins de reinscrição/renovação de certificado. Se essa opção não for especificada, a chave RSA atual será usada.

Inscrição automática em ação

Conclua estes passos para verificar o recurso de inscrição automática:

1. Insira o comando **crypto pki authenticate** para autenticar manualmente o ponto de confiança no roteador do cliente:

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

   Note: Para obter mais informações sobre esse comando, consulte a Referência de Comandos de Segurança do Cisco IOS.
   Depois de inserir o comando, uma saída semelhante a esta deverá aparecer:

   ```
   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. Digite **yes** para aceitar o certificado CA no roteador cliente. Em seguida, um temporizador **RENEW** começa no roteador:

   ```
   Client-1#show crypto pki timer
   PKI Timers
   | 0.086
   | 0.086 RENEW cvo-pki
   | 9:51.366 SESSION CLEANUP
   ```
3. Quando o temporizador **RENEW** chegar a zero, o roteador do cliente se inscreve automaticamente na CA para obter seu certificado de identidade. Quando o certificado for recebido, insira o comando **show crypto pki certificate** para exibi-lo:

   ```
   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
```

A **data de renovação** é **09:30:08** e é calculada conforme mostrado aqui:

hora de início + (%renovação de ID_cert_lifetime)

Ou

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

Os temporizadores PKI refletem o mesmo:

```
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. Quando o temporizador **RENEW** expirar, o roteador se registra novamente com a CA para obter um novo certificado de ID. Após a renovação de um certificado, insira o comando **show crypto pki cert** para exibir o novo 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 não há mais uma *data de renovação*; em vez disso, um temporizador **SHADOW** começa:

```
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
```

Aqui está a lógica do processo:

- Se a data de término do certificado de ID **não for igual** à data de término do **certificado de AC**, calcule uma data de renovação com base na porcentagem de inscrição automática e inicie o **cronômetro de** renovação.
- Se a data de término do certificado de **ID for igual** à data de término do **certificado de AC**, não será necessário qualquer processo de renovação, uma vez que o certificado de ID atual é válido apenas enquanto o certificado de AC atual for válido. Em vez disso, um temporizador **SHADOW** é iniciado.

Esse temporizador também é calculado com base na porcentagem mencionada no comando **autoenroll**. Por exemplo, considere as datas de validade do certificado de ID renovado que são mostradas no exemplo 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
```

O tempo de vida deste certificado é de 16 minutos. Portanto, o temporizador de rollover (isto é, o

temporizador SHADOW) é de 70% de 16 minutos, o que equivale a aproximadamente 11 minutos. Esse cálculo implica que o roteador inicia solicitações para seus certificados de sombra/rollover em [09:30:09 + 00:11:00] = 09:41:09, que corresponde ao temporizador PKI SHADOW mostrado anteriormente neste 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
```

Substituição automática em ação

Esta seção descreve o recurso de substituição automática em ação.

No Cisco IOS CA Server

Quando o temporizador SHADOW expira, o certificado de rollover aparece no roteador 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
```

No roteador cliente

Conforme descrito anteriormente neste documento, o recurso de inscrição automática começou um temporizador SHADOW no roteador do cliente. Quando o temporizador SHADOW expira, o recurso de inscrição automática permite que o roteador solicite ao servidor CA o certificado *CA de rollover/sombra*. Uma vez recebido, ele também consulta seu certificado *de ID de sobreposição/sombra*. Como resultado, o roteador tem dois pares de certificados: um par atual e o outro par que contém os certificados 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
```

Observe a validade do certificado de ID de rollover:

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

O tempo de vida do certificado é de apenas quatro minutos (em vez dos 20 minutos esperados, conforme configurado no servidor de CA do Cisco IOS). De acordo com o servidor da CA do Cisco IOS, o tempo de vida do certificado de ID *absoluto* deve ser de 20 minutos (o que significa que, para um determinado roteador cliente, a soma dos tempos de vida dos certificados de ID (atual + sombra) emitidos para ele não deve ser superior a 20 minutos).

Este processo é descrito aqui:

- Aqui está a validade do certificado de ID atual no roteador:

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

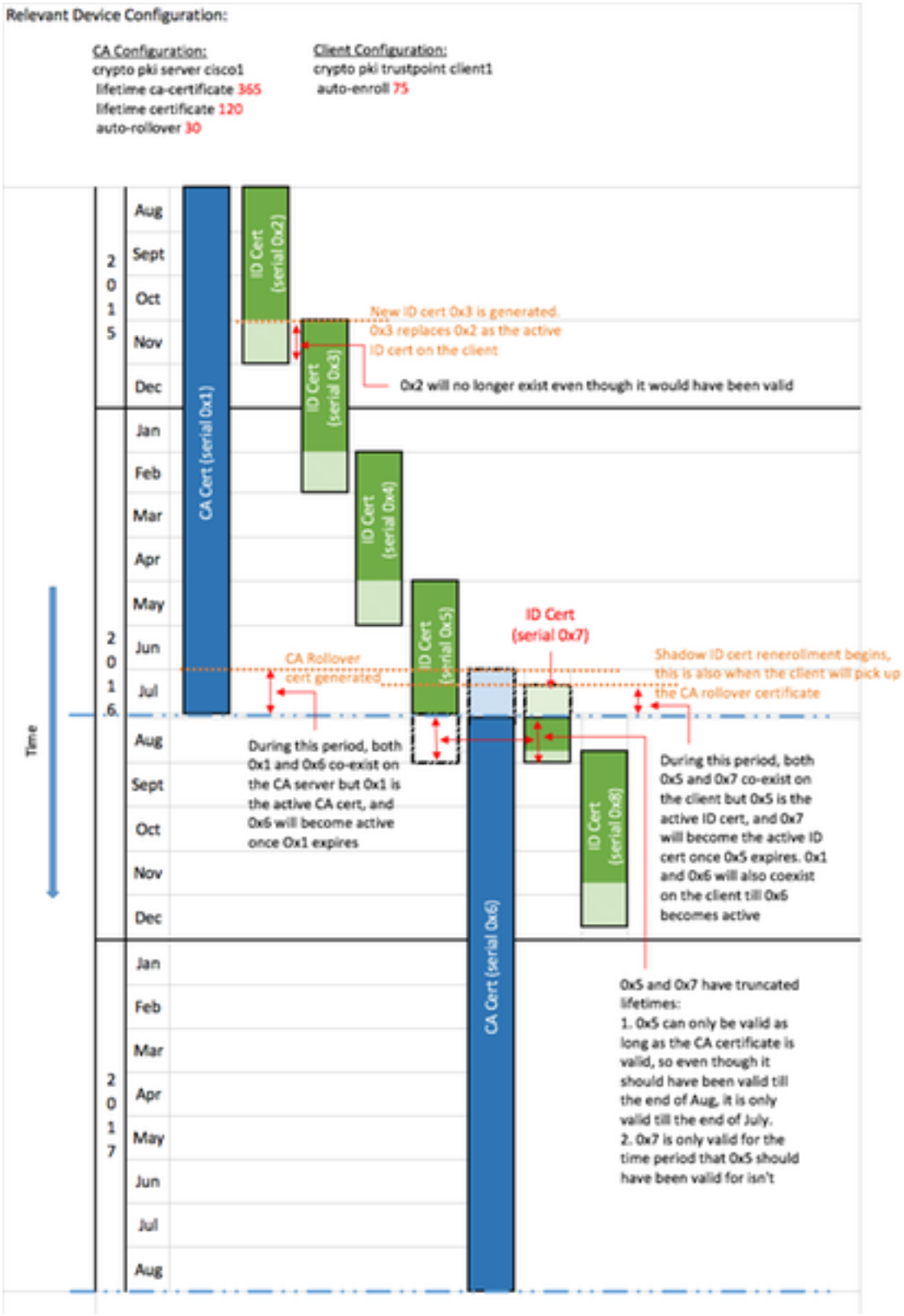
  Portanto, o *current_id_cert_lifetime* é de 16 minutos.
- Aqui está a validade do certificado de ID de rollover:

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

  Portanto, o *rollover_id_cert_lifetime* é de quatro minutos.
- De acordo com o Cisco IOS, quando [current_id_cert_lifetime] é adicionado a

[rollover_id_cert_lifetime], ele deve ser igual a [total_id_cert_lifetime]. Isso é verdade neste caso.

Exemplo de cronograma de PKI com rollover e inscrição



Considerações importantes

- Os temporizadores PKI exigem um relógio autoritativo para funcionarem corretamente. A

Cisco recomenda que você use o NTP para sincronizar relógios entre os roteadores clientes e o roteador da CA do Cisco IOS. Na ausência de NTP, o relógio do sistema/hardware no roteador pode ser usado. Para obter informações sobre como configurar o relógio de hardware e torná-lo autoritativo, consulte o Guia Básico de Configuração de Gerenciamento do Sistema, Cisco IOS versão 12.4T.

- Após o recarregamento de um roteador, a sincronização do NTP frequentemente leva alguns minutos. No entanto, os temporizadores PKI são estabelecidos quase imediatamente. A partir das versões 15.2(3.8)T e 15.2(4)S, os temporizadores PKI são automaticamente reavaliados depois que o NTP é sincronizado.

- Os temporizadores PKI não são absolutos; são baseados no *tempo restante* e, portanto, são recalculados após uma reinicialização. Por exemplo, suponha que o roteador cliente tenha um certificado de ID válido por 100 dias e que o recurso de inscrição automática esteja definido como 80%. Em seguida, espera-se que a reinscrição ocorra após o 80º dia. Se o roteador for recarregado no 60º dia, ele inicializará e recalculará o temporizador PKI como mostrado aqui: (*tempo restante*) * (*%autoinscrição*) = (100-60) * 80% = 32 dias.

  Portanto, a reinscrição ocorre no [60 + 32] = 92º dia.

- Quando você configura os temporizadores de autoinscrição e de rolagem automática, é importante configurá-los com valores que permitam a disponibilidade do certificado CA SHADOW no servidor PKI quando o cliente PKI solicitar um. Isso ajuda a reduzir possíveis falhas de serviços PKI em um ambiente de grande escala.

Informações Relacionadas

- Implementação da segurança do Cisco IOS com um white paper de infraestrutura de chave pública
- Infraestrutura de chave pública: Documentação sobre benefícios e recursos de implantação
- Guia de configuração da infraestrutura de chave pública
- Suporte Técnico e Documentação - Cisco Systems