Auto-enroll, auto-rollover, et temporisateurs de PKI IOS

Contenu

Introduction

Ce document décrit comment les exécutions d'Infrastructure à clés publiques (PKI) de Cisco IOS® de l'Auto-inscription et de l'auto-rollover fonctionnent et comment les temporisateurs respectifs de PKI sont calculés pour ces exécutions.

Les Certificats ont réparé des vies et expirent à un certain point. Si les Certificats sont utilisés pour l'authentification pour une solution VPN (par exemple), l'échéance de ces Certificats mène aux échecs d'authentification possibles qui ont comme conséquence la perte de connectivité VPN entre les points finaux. Afin d'éviter cette question, ces deux mécanismes sont disponibles pour le renouvellement automatique de certificat :

- Auto-inscription pour le client/routeurs en étoile
- Auto-rollover pour le routeur de serveur de l'autorité de certification (CA)

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- PKI et le concept de la confiance
- Configuration de base de CA sur des Routeurs

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Terminologie

Auto-inscription

Quand un certificat sur un périphérique d'extrémité est sur le point d'expirer, l'Auto-inscription obtient un nouveau certificat sans interruption. Quand l'Auto-inscription est configurée, le client/routeur en étoile peut demander un nouveau certificat à un moment donné avant que son propres moyens certificat (connu sous le nom de son identité ou certificat d'ID) expire.

auto-rollover

Ce paramètre décide quand le serveur de certificat (CS) génère son certificat inversé (de shadow) ; si la commande est sélectionnée sous la configuration de CS sans n'importe quel argument, le délai par défaut est de 30 jours.

> Remarque: Pour les exemples dans ce document, la valeur de ce paramètre est de *10 minutes*.

Quand un certificat sur le serveur CA est sur le point d'expirer, l'auto-rollover permet au CA d'obtenir un nouveau certificat sans interruption. Quand l'auto-rollover est configuré, le routeur CA peut générer un nouveau certificat à un moment donné avant que son propre certificat expire. Le nouveau certificat, qui s'appelle le *shadow* ou le certificat *inversé*, devient actif au moment précis que le certificat de CA en cours expire.

Avec l'utilisation des deux caractéristiques qui sont mentionnées dans la section d'introduction de ce document, le déploiement de PKI devient automatisé et permet au périphérique de rai ou de client pour obtenir un shadow/certificat d'identité inversé et ombrager/certificat de CA inversé avant l'échéance en cours de certificat de CA. De cette façon, il peut transition sans interruption aux nouveaux Certificats d'ID et CA quand ses Certificats en cours d'ID et CA expirent.

Ca-certificat de vie

Ce paramètre spécifie la vie du certificat de CA. La valeur de ce paramètre peut être spécifiée en quelques jours/heures/minutes.

> Remarque: Pour les exemples dans ce document, la valeur de ce paramètre est de *30 minutes*.

certificat de vie

Ce paramètre spécifie la vie du certificat d'identité qui est délivré par le routeur CA. La valeur de ce paramètre peut être spécifiée en quelques jours/heures/minutes.

> Remarque: Pour les exemples dans ce document, la valeur de ce paramètre est de *20 minutes*

Configurez

> Remarque: De plus petites valeurs de temporisateur de PKI pour la *vie*, l'*auto-rollover*, et l'*auto-enroll* sont utilisées dans ce document afin d'illustrer les concepts principaux d'auto-enroll et d'auto-rollover. Dans un environnement de réseau vivant, Cisco recommande que vous utilisiez les vies par défaut pour ces paramètres.

> **Conseil** : Tous les événements basés sur temporisateur de PKI, tels que le *renversement* et le *reenrollment*, peuvent être affectés s'il n'y a aucune source temporelle bien fondée. Pour cette raison, Cisco recommande que vous configuriez le Protocole NTP (Network Time Protocol) sur tous les Routeurs ce PKI de peform.

Configuration du serveur du Cisco IOS CA

Cette section fournit un configuratinon d'exemple pour le serveur du Cisco IOS CA.

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

> Remarque: La valeur qui est spécifiée avec la commande d'**auto-rollover** est le nombre de jours/d'heures/de minutes *avant la date de fin du certificatethat du courant CA que le* certificat inversé est généré. Par conséquent, si un certificat de CA est valide de 12:00 à 12:30, puis l'**auto-rollover 0 0 10** implique que le certificat de CA inversé est généré autour de 12:20.

Sélectionnez la **crypto** commande de **certificat de PKI d'exposition** afin de vérifier la configuration sur le serveur du Cisco IOS CA :

```
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
```

Basé sur cette sortie, le routeur inclut un certificat de CA qui est valide de 9:16 à IST nov. 25, 2012 de 9:46. Puisque l'auto-rollover est configuré pendant 10 minutes, on s'attend à ce que le shadow/certificat inversé soit généré par *9.36 IST* nov. 25, 2012.

Afin de confirmer, sélectionnez la **crypto** commande de **temporisateur de PKI d'exposition** :

```
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
```

Basé sur cette sortie, la **crypto** commande de **temporisateur de PKI d'exposition** a été émise à 9.19 IST, et on s'attend à ce que le shadow/certificat inversé soit généré dans un délai de 16.43 minutes :

[09:19:22 + 00:16:43] = **09:36:05**, qui est [end-date_of_current_CA_cert - auto_rollover_timer] ; c'est-à-dire, [09:46:05 - 00:10:00] = **09:36:05**.

Configuration de client/routeur en étoile

Cette section fournit un exemple de configuration pour le client/routeur en étoile.

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

> Remarque: Les commandes enables d'**auto-enroll la** caractéristique d'Auto-inscription sur le routeur. La syntaxe de commande est la suivante : **auto-enroll** [*val%*] [*régénéré*].

Dans la sortie précédente, la caractéristique d'auto-enroll est spécifiée en tant que 70% ; c'est-à-dire, à 70% de **[vie de current_ID_cert]**, de routeur les reenrolls automatiquement avec le CA.

> **Conseil** : Cisco recommande que vous placiez la valeur d'auto-enroll à 60% ou plus afin de s'assurer que les temporisateurs de PKI fonctionnent correctement.

L'option *régénérée* mène à la création d'une nouvelle clé de Rivest-Shamir-Addleman (RSA) pour des buts de reenrollment/renouvellement de certificat. Si cette option n'est pas spécifiée, la clé RSA en cours est utilisée.

Auto-inscription dans l'action

Terminez-vous ces étapes afin de vérifier la caractéristique d'Auto-inscription :

1. Sélectionnez la commande de **crypto pki authenticate** afin d'authentifier manuellement le point de confiance sur le routeur client :

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

   Remarque: Pour plus d'informations sur cette commande, référez-vous à la référence de commandes de Cisco IOS Security.
   Une fois que vous sélectionnez la commande, un résultat semblable à ceci devrait apparaître :

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

2. Type **oui** afin de recevoir le certificat de CA sur le routeur client. Puis, un temporisateur de **RENOUVELER** commence sur le routeur :

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

3. Une fois le temporisateur de **RENOUVELER** atteint zéro, le routeur client s'inscrit automatiquement avec le CA afin d'obtenir son certificat d'identité. Une fois le certificat est reçu, sélectionne la **crypto** commande de **certificat de PKI d'exposition** afin de la visualiser :

   ```
   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 date de renouveler est **09:30:08** et est calculée comme affiché ici :

start-time + (%renewal d'ID_cert_lifetime)

Ou

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

Les temporisateurs de PKI reflètent la même chose :

```
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. Une fois le temporisateur de **RENOUVELER** expire, les reenrolls de routeur avec le CA afin d'obtenir un nouveau certificat d'ID. Après qu'un renouvellement de certificat se soit produit, sélectionnez la **crypto** commande de **CERT de PKI d'exposition** afin de visualiser le nouveau certificat d'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
```

Notez qu'il n'y a plus une *date de renouveler* ; au lieu de cela, un temporisateur de SHADOW commence :

```
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
```

Voici la logique de processus :

- Si la date de fin du certificat d'ID n'est pas égale à la date de fin du certificat de CA, alors calculez une renouveler-date basée sur le pourcentage d'auto-enroll et mettez en marche le temporisateur de RENOUVELER.

- Si la date de fin du certificat d'ID est égale à la date de fin du certificat de CA, alors aucun processus de renouvellement n'est nécessaire puisque le certificat en cours d'ID est valide seulement tant que le certificat de CA en cours est valide. Au lieu de cela, un temporisateur de SHADOW est démarré.

Ce temporisateur est également calculé basé sur le pourcentage mentionné dans la commande d'auto-enroll. Par exemple, considérez les dates de validité du certificat renouvelé d'ID qui sont affichées dans l'exemple précédent :

```
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 vie de ce certificat est de 16 minutes. Par conséquent, le temporisateur inversé (c'est-à-dire, le temporisateur de SHADOW) est 70% de 16 minutes, qui égale approximativement 11 minutes. Ce calcul implique que le routeur commence des demandes de son shadow/Certificats inversés à [09:30:09 + 00:11:00] = 09:41:09, qui correspond au temporisateur de SHADOW de PKI affiché précédemment dans ce document :

```
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
```

Auto-rollover dans l'action

Cette section décrit la caractéristique d'auto-rollover dans l'action.

Sur le serveur du Cisco IOS CA

Quand le temporisateur de SHADOW expire, le certificat inversé apparaît sur le routeur 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
```

Au routeur client

Comme décrit précédemment dans ce document, la caractéristique d'Auto-inscription a commencé un temporisateur de SHADOW sur le routeur client. Quand le temporisateur de SHADOW expire, la caractéristique d'Auto-inscription permet au routeur de demander le serveur CA pour le *renversement/certificat de CA de shadow*. Une fois que reçu, il questionne pour son *renversement/*certificat *ID de shadow* aussi bien. En conséquence, le routeur a deux paires de Certificats : une paire qui est en cours et l'autre paire qui contient le renversement/shadow délivre un certificat :

```
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
```

Notez la validité du certificat inversé d'ID :

```
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
```

La vie de certificat est juste quatre minutes (au lieu des 20 minutes prévues, comme configurées sur le serveur de Cisco IOS CA). Par serveur du Cisco IOS CA, la vie *absolue de* certificat d'ID devrait être de 20 minutes (qui signifie, pour un routeur client indiqué, la somme des vies des Certificats d'ID (courant + shadow) fournis à elle ne doit pas être plus grande que 20 minutes).

Ce processus est encore décrit ici :

- Voici la validité du certificat en cours d'ID sur le routeur :

```
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
```

Par conséquent, le *current_id_cert_lifetime* est de 16 minutes.

- Voici la validité du certificat inversé d'ID :

```
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

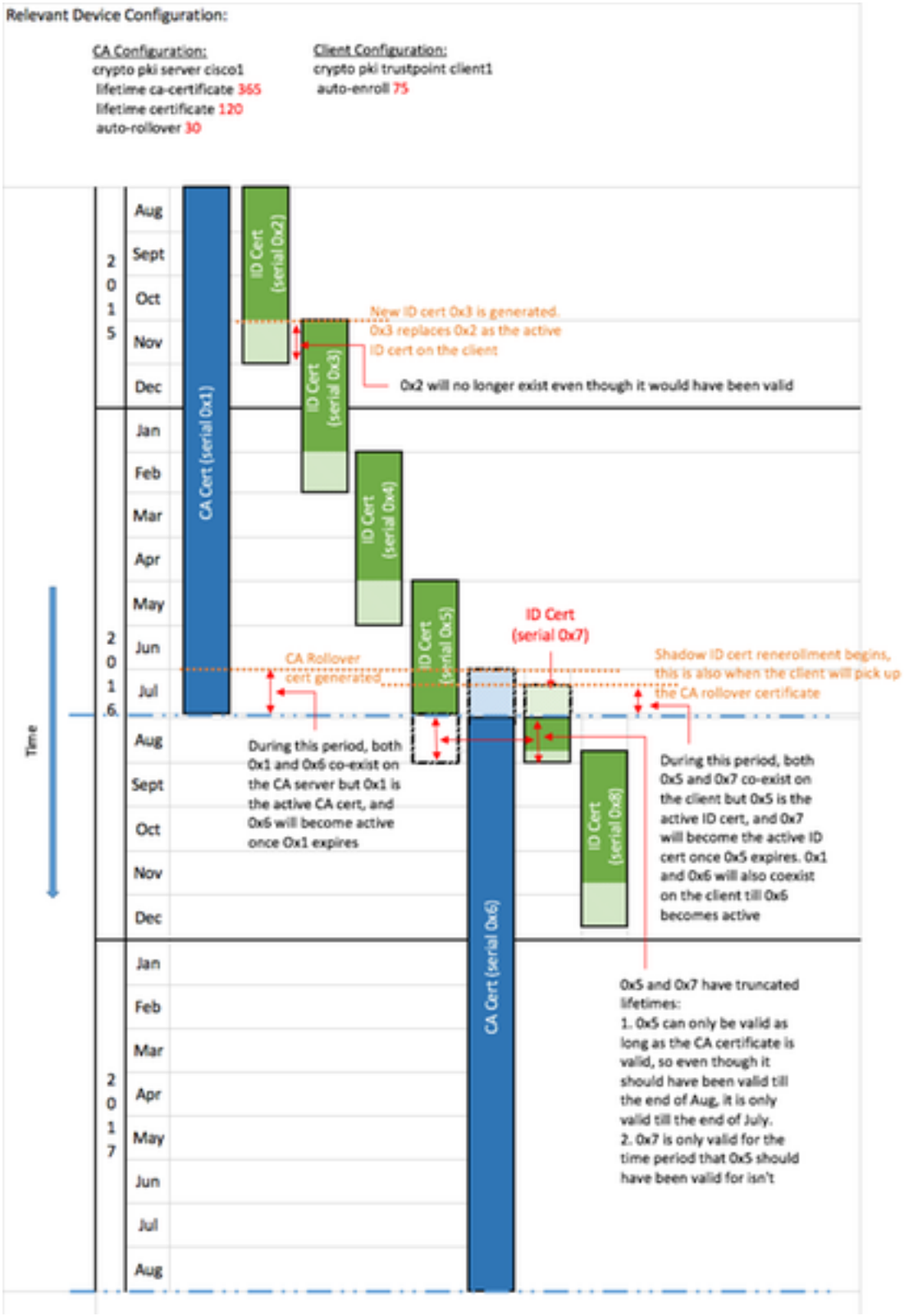
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012

```
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

Par conséquent, le *rollover_id_cert_lifetime* est de quatre minutes.

- Par Cisco IOS, quand [current_id_cert_lifetime] est ajouté au [rollover_id_cert_lifetime], il doit égaler [total_id_cert_lifetime]. C'est vrai dans ce cas.

Chronologie de PKI d'échantillon avec le renversement et l'inscription



Importantes considérations

- Les temporisateurs de PKI exigent d'une horloge bien fondée afin de fonctionner correctement. Cisco recommande que vous employiez le NTP afin de synchroniser des horloges entre les routeurs client et le routeur du Cisco IOS CA. Faute de NTP, l'horloge de système/matériel sur le routeur peut être utilisée. Pour les informations sur la façon dont configurer le matériel synchronisez-et rendez-le bien fondé, se rapportent au guide de configuration de base de gestion du système, Cisco IOS version 12.4T.

- Sur la recharge d'un routeur, la synchronisation du NTP prend souvent quelques minutes. Cependant, les temporisateurs de PKI sont établis presque immédiatement. En date des versions 15.2(3.8)T et 15.2(4)S, les temporisateurs de PKI sont automatiquement réévalués après que le NTP soit synchronisé.

- Les temporisateurs de PKI ne sont pas absolus ; ils sont basés sur le *temps restant* et sont donc recalculés après une réinitialisation. Par exemple, supposez que le routeur client a un certificat d'ID qui est valable 100 jours et la caractéristique d'auto-enroll est placée à 80%. Puis, on s'attend à ce que le reenrollment se produise après le quatre-vingtième jour. Si le routeur est rechargé le soixantième jour, il initialise et recalcule le temporisateur de PKI comme affiché ici : (*temps restant*) * (*%auto-enroll*) = (100-60) * 80% = 32 jours.

  Par conséquent, le reenrollment se produit sur [60 + 32] = le quatre-vingt-douzième jour.

- Quand vous configurez l'auto-enroll et l'automatique-rollovertimers, il est important de les configurer avec les valeurs qui permettent la Disponibilité de certificat de CA de SHADOW sur le serveur de PKI quand le client de PKI demande un. Ceci aide à atténuer des pannes potentielles de services de PKI dans un environnement de grande puissance.

Informations connexes

- Déployer le Cisco IOS Security avec Livre blanc d'infrastructure de clé publique
- Infrastructure de clé publique : Livre blanc d'avantages et de caractéristiques de déploiement
- Guide de configuration d'infrastructure de clé publique
- Support et documentation techniques - Cisco Systems