Inscription automatique, transfert automatique et minuteurs de l'ICP IOS

Contenu

Introduction

Ce document décrit le fonctionnement de l'infrastructure à clé publique (PKI) de Cisco IOS® d'inscription automatique et de substitution automatique et comment les temporisateurs PKI respectifs sont calculés pour ces opérations.

Les certificats ont une durée de vie fixe et expirent à un moment donné. Si les certificats sont utilisés à des fins d'authentification pour une solution VPN (par exemple), l'expiration de ces certificats entraîne d'éventuels échecs d'authentification qui entraînent une perte de connectivité VPN entre les points d'extrémité. Afin d'éviter ce problème, ces deux mécanismes sont disponibles pour le renouvellement automatique des certificats :

- Inscription automatique pour les routeurs client/satellite
- Transfert automatique pour le routeur serveur de l'autorité de certification (CA)

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- L'ICP et le concept de confiance
- Configuration de base de CA sur les routeurs

Components Used

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. 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.

Terminologie

inscription automatique

Lorsqu'un certificat sur un périphérique final est sur le point d'expirer, l'inscription automatique obtient un nouveau certificat sans interruption. Lorsque l'inscription automatique est configurée, le routeur client/satellite peut demander un nouveau certificat avant l'expiration de son propre certificat (appelé certificat d'identité ou d'ID).

renversement automatique

Ce paramètre décide quand le serveur de certificats (CS) génère son certificat de renversement (shadow) ; si la commande est entrée dans la configuration CS sans argument, l'heure par défaut est 30 jours.

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

Lorsqu'un certificat sur le serveur AC est sur le point d'expirer, la substitution automatique permet à l'AC d'obtenir un nouveau certificat sans interruption. Lorsque la substitution automatique est configurée, le routeur AC peut générer un nouveau certificat avant l'expiration de son propre certificat. Le nouveau certificat, appelé le certificat *fantôme* ou *inversé*, devient actif au moment précis où le certificat CA actuel expire.

Avec l'utilisation des deux fonctionnalités mentionnées dans la section Introduction de ce document, le déploiement de l'ICP devient automatisé et permet au périphérique satellite ou client d'obtenir un certificat d'identité de substitution/de substitution et un certificat d'autorité de certification de substitution/de substitution avant l'expiration du certificat d'autorité de certification actuel. De cette façon, il peut passer sans interruption aux nouveaux certificats d'ID et d'AC lorsque son ID et ses certificats d'AC actuels expirent.

cycle de vie ca-certificate

Ce paramètre spécifie la durée de vie du certificat de l'autorité de certification. La valeur de ce paramètre peut être spécifiée en jours/heures/minutes.

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

certificat de durée de vie

Ce paramètre spécifie la durée de vie du certificat d'identité émis par le routeur de l'autorité de

certification. La valeur de ce paramètre peut être spécifiée en jours/heures/minutes.

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

Configuration

> **Remarque** : Les valeurs de minuteur PKI plus petites pour *la durée de vie*, le *basculement automatique* et l'*inscription automatique* sont utilisées dans ce document afin d'illustrer les concepts clés d'inscription automatique et de transfert automatique. Dans un environnement de réseau en direct, Cisco vous recommande d'utiliser les durées de vie par défaut pour ces paramètres.

> **Conseil** : tous les événements basés sur le minuteur PKI, tels que le *basculement* et le *réinscription*, peuvent être affectés s'il n'y a pas de source temporelle faisant autorité. C'est pourquoi Cisco vous recommande de configurer le protocole NTP (Network Time Protocol) sur tous les routeurs qui exécutent l'ICP.

Configuration du serveur Cisco IOS CA

Cette section fournit un exemple de configuration pour le serveur 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:
```

> **Remarque** : La valeur spécifiée avec la commande **auto-renversement** est le nombre de jours/heures/minutes *avant la date de fin du* certificat *CA actuel* que le certificat de renversement est généré. Par conséquent, si un certificat d'autorité de certification est valide de 12 h 00 à 12 h 30, le **transfert automatique 0 0 10** implique que le certificat d'autorité de certification inversé est généré vers 12 h 20.

Entrez la commande **show crypto pki certificate** afin de vérifier la configuration sur le serveur 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
```

Sur la base de ce résultat, le routeur inclut un certificat CA valide de 9:16 à 9:46 IST 25 novembre 2012. Étant donné que le transfert automatique est configuré pour 10 minutes, le certificat de transfert/transfert doit être généré d'ici le 25 novembre 2012 *9.36 IST*.

Afin de confirmer, entrez la commande **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
```

Sur la base de ce résultat, la commande **show crypto pki timer** a été émise à l'adresse 9.19 IST, et le certificat shadow/rollover devrait être généré dans les 16.43 minutes suivantes :

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

Configuration du routeur client/satellite

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

```
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
```

> **Remarque** : la commande **auto-enroll** active la fonction d'inscription automatique sur le routeur. La syntaxe de la commande est : **auto-enroll** [*val%*] [*régénération*].

Dans le résultat précédent, la fonction d'inscription automatique est spécifiée comme 70 %; c'est-à-dire qu'à 70 % de la **[durée de vie de current_ID_cert]**, le routeur s'inscrit automatiquement à nouveau avec l'autorité de certification.

> **Conseil** : Cisco vous recommande de définir la valeur de l'inscription automatique à 60 % ou plus afin de vous assurer que les temporisateurs PKI fonctionnent correctement.

L'option *de régénération* conduit à la création d'une nouvelle clé Rivest-Shamir-Addleman (RSA) pour la réinscription/renouvellement de certificat. Si cette option n'est pas spécifiée, la clé RSA actuelle est utilisée.

Inscription automatique en action

Complétez ces étapes afin de vérifier la fonctionnalité d'inscription automatique :

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

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

   Note: Pour plus d'informations sur cette commande, référez-vous à Référence des commandes de sécurité Cisco IOS.
   Une fois la commande saisie, une sortie similaire à celle-ci doit apparaître :

```
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. Tapez **yes** afin d'accepter le certificat CA sur le routeur client. Ensuite, un minuteur **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 que le minuteur **RENEW** atteint zéro, le routeur client s'inscrit automatiquement avec l'autorité de certification afin d'obtenir son certificat d'identité. Une fois le certificat reçu, entrez la commande **show crypto pki certificate** afin de le 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 renouvellement** est **09:30:08** et est calculée comme indiqué ici :

start-time + (%renouvellement de ID_cert_lifetime)

OU

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

Les temporisateurs PKI reflètent les mêmes :

```
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 minuteur **RENOUVELER** expiré, le routeur s'inscrit de nouveau auprès de l'autorité de certification afin d'obtenir un nouveau certificat d'ID. Après un renouvellement de certificat, entrez la commande **show crypto pki cert** afin d'afficher 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 de *date de renouvellement* ; au lieu de cela, un compteur **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 l'**autorité de certification**, calculez une date de renouvellement en fonction du pourcentage d'inscription automatique et démarrez le **RENOUVEAU** temporisateur.
- Si la date de fin du certificat **d'ID est égale** à la date de fin du certificat de l'**Autorité de certification**, aucun processus de renouvellement n'est nécessaire puisque le certificat d'ID actuel n'est valide que tant que le certificat de l'Autorité de certification actuel est valide. À la place, un minuteur **SHADOW** est démarré.

Ce compteur est également calculé en fonction du pourcentage mentionné dans la commande **auto-enroll**. Par exemple, considérez les dates de validité du certificat d'ID renouvelé qui sont indiquées dans l'exemple précédent :

```
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 durée de vie de ce certificat est de 16 minutes. Par conséquent, le compteur de renversement (c'est-à-dire le compteur SHADOW) est de 70 % sur 16 minutes, ce qui équivaut à environ 11 minutes. Ce calcul implique que le routeur commence à demander ses certificats de substitution/ombre à [09:30:09 + 00:11:00] = 09:41:09, ce qui correspond au compteur PKI SHADOW indiqué 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
```

Transfert automatique en action

Cette section décrit la fonction de renversement automatique en action.

Sur le serveur CA Cisco IOS

Lorsque le minuteur SHADOW expire, le certificat de renversement 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 niveau du routeur client

Comme décrit précédemment dans ce document, la fonction d'inscription automatique a démarré un minuteur SHADOW sur le routeur client. Lorsque le minuteur SHADOW expire, la fonction d'inscription automatique permet au routeur de demander au serveur AC le certificat *de* l'*autorité de certification inversée/cachée*. Une fois reçu, il demande également son certificat *de substitution/d'ID d'ombre*. Par conséquent, le routeur possède deux paires de certificats : une paire qui est actuelle et l'autre qui contient les certificats de substitution/d'ombre :

```
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 d'ID de substitution :

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

La durée de vie du certificat est de seulement quatre minutes (au lieu des 20 minutes prévues, telles que configurées sur le serveur AC Cisco IOS). Selon le serveur AC Cisco IOS, la durée de vie *absolue* du certificat d'ID doit être de 20 minutes (ce qui signifie que, pour un routeur client donné, la somme des durées de vie des certificats d'ID (actuels + fantômes) qui lui sont délivrés ne doit pas être supérieure à 20 minutes).

Ce processus est décrit plus en détail ici :

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

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

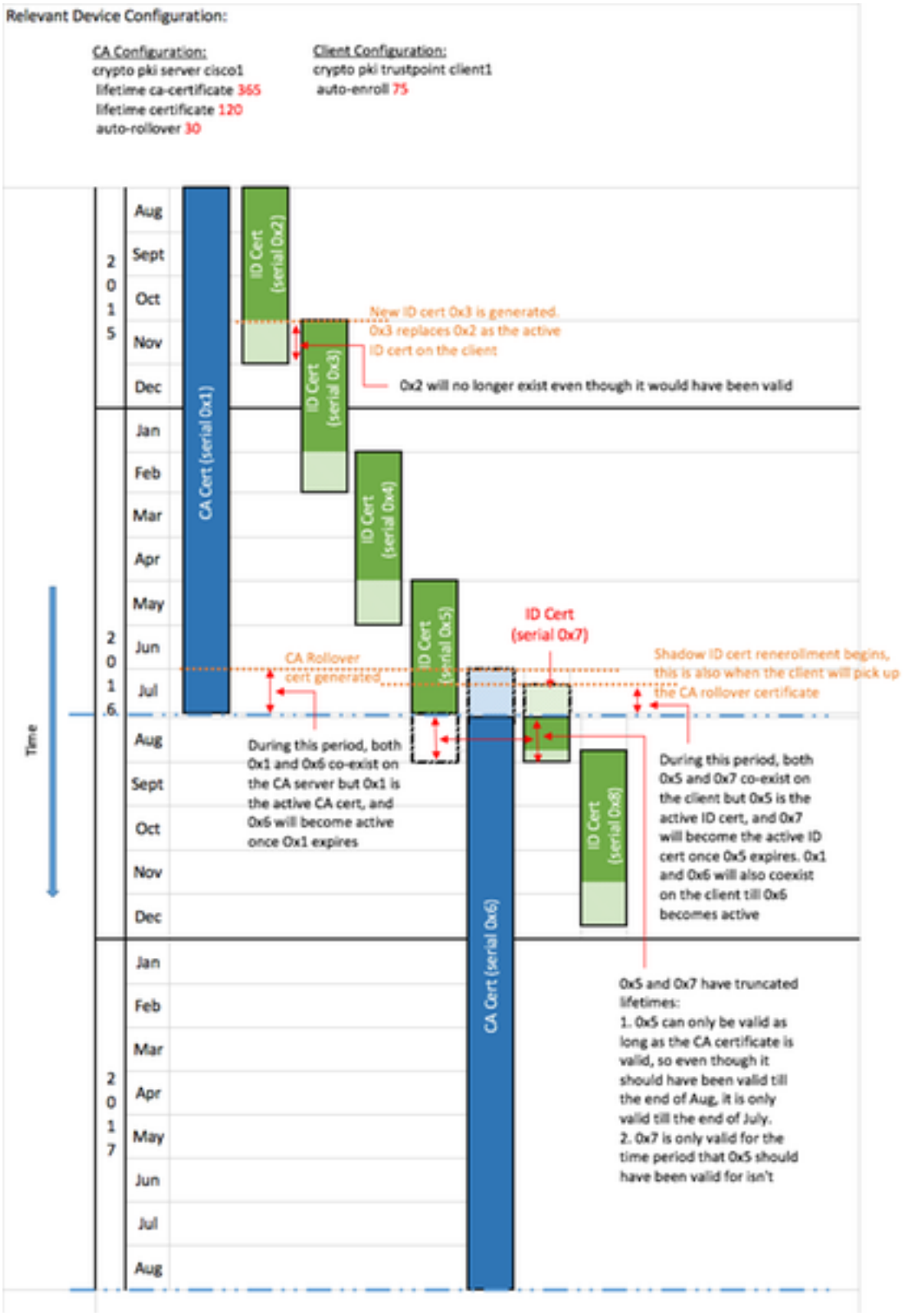
  Par conséquent, la *durée de vie actuelle_id_cert_lifetime* est de 16 minutes.

- Voici la validité du certificat d'ID de transfert :

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

  Par conséquent, la *durée de vie de rollover_id_cert_lifetime* est de quatre minutes.
- Selon Cisco IOS, lorsque [current_id_cert_lifetime] est ajouté à [rollover_id_cert_lifetime], il doit être égal à [total_id_cert_lifetime]. C'est vrai dans ce cas.

Exemple de scénario PKI avec transfert et inscription



Considérations importantes

- Les minuteurs PKI nécessitent une horloge faisant autorité pour fonctionner correctement. Cisco vous recommande d'utiliser NTP afin de synchroniser les horloges entre les routeurs client et le routeur CA Cisco IOS. En l'absence de NTP, l'horloge système/matérielle du routeur peut être utilisée. Pour plus d'informations sur la façon de configurer l'horloge matérielle et de faire autorité, reportez-vous au Guide de configuration de la gestion du système de base, Cisco IOS version 12.4T.

- Lors du rechargement d’un routeur, la synchronisation du NTP prend souvent quelques minutes. Cependant, les temporisateurs PKI sont établis presque immédiatement. Depuis les versions 15.2(3.8)T et 15.2(4)S, les temporisateurs PKI sont automatiquement réévalués après la synchronisation de NTP.

- Les temporisateurs PKI ne sont pas absolus ; ils sont basés sur le *temps restant* et sont donc recalculés après un redémarrage. Par exemple, supposons que le routeur client possède un certificat d'ID valide pendant 100 jours et que la fonction d'inscription automatique est définie sur 80 %. Ensuite, il est prévu que la réinscription ait lieu après le 80e jour. Si le routeur est rechargé le 60e jour, il démarre et recalcule le compteur PKI comme indiqué ici : (*temps restant*) * (*%auto-inscription*) = (100-60) * 80 % = 32 jours.

  Par conséquent, la réinscription a lieu le [60 + 32] = 92e jour.

- Lorsque vous configurez les temporisateurs d'inscription automatique et de résolution automatique, il est important de les configurer avec des valeurs qui autorisent la disponibilité des certificats de l'autorité de certification SHADOW sur le serveur PKI lorsque le client PKI en demande une. Cela permet d'atténuer les défaillances potentielles des services PKI dans un environnement à grande échelle.

Informations connexes

- Déploiement de la sécurité Cisco IOS avec un livre blanc sur l'infrastructure à clé publique
- Infrastructure à clé publique : Livre blanc sur les avantages et les fonctionnalités du déploiement
- Guide de configuration de l'infrastructure à clé publique
- Support et documentation techniques - Cisco Systems