التسجيل التلقائي ل IOS PKI، وإعادة التحميل التلقائي، ومؤقتات الوقت

المحتويات

المقدمة

يوضح هذا المستند كيفية حساب عمليات Cisco IOS® Public Key Infrastructure (PKI) للتسجيل التلقائي وعمل إعادة التوجيه التلقائي وكيفية حساب وحدات توقيت PKI المقابلة لهذه العمليات.

تحتوي الشهادات على فترات حياة ثابتة وتنتهي عند نقطة ما. إذا تم إستخدام الشهادات لأغراض المصادقة لحل شبكة VPN (على سبيل المثال)، يؤدي انتهاء صلاحية هذه الشهادات إلى حالات فشل مصادقة محتملة ينتج عنها فقد اتصال VPN بين نقاط النهاية. لتجنب هذه المشكلة، توفر هاتان الآليتان للتجديد التلقائي للشهادة:

- التسجيل التلقائي لموجهات العميل/المتكلم
- التمرير التلقائي لموجه خادم المرجع المصدق (CA)

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- PKI ومفهوم الثقة
- التكوين الأساسي ل CA على الموجهات

المكونات المستخدمة

ال يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

مصطلحات

التسجيل التلقائي

عندما تكون الشهادة على الجهاز الطرفي على وشك الانتهاء، يحصل التسجيل التلقائي على شهادة جديدة دون انقطاع. عند تكوين التسجيل التلقائي، يمكن لموجه العميل/المتحدث طلب شهادة جديدة في وقت ما قبل انتهاء صلاحية شهادته (المعروفة بشهادة الهوية أو معرف الهوية).

تمرير تلقائي

تحدد هذه المعلمة متى يقوم خادم الشهادة (CS) بإنشاء شهادة المرور (الظل) الخاصة به، وإذا تم إدخال الأمر تحت تكوين CS بدون أي وسيطة، يكون الوقت الافتراضي 30 يوما.

> **ملاحظة**: بالنسبة للأمثلة الواردة في هذا المستند، تكون قيمة هذه المعلمة *10 دقائق*.

عندما تكون الشهادة على خادم CA على وشك الانتهاء، فإن التمرير التلقائي يمكن CA من الحصول على شهادة جديدة دون انقطاع. عند تكوين التمرير التلقائي، يمكن لموجه CA إنشاء شهادة جديدة في وقت ما قبل انتهاء صلاحية شهادته. تصبح الشهادة الجديدة، والتي تسمى شهادة *الظل* أو *المرور*، نشطة في اللحظة الدقيقة التي تنتهي فيها صلاحية شهادة المرجع المصدق الحالية.

مع إستخدام الميزتين المذكورتين في قسم المقدمة من هذا المستند، يصبح نشر PKI تلقائيا ويسمح للجهاز المتكلم أو العميل بالحصول على شهادة هوية ظل/إعادة توجيه وشهادة مرجع مصدق (CA) الظل/إعادة التوجيه قبل انتهاء صلاحية شهادة CA الحالية. بهذه الطريقة، يمكنها الانتقال بدون مقاطعة إلى المعرف الجديد وشهادات المرجع المصدق عندما تنتهي صلاحية شهاداتها الحالية للمعرف والمصادقة.

شهادة المرجع المصدق مدى الحياة

تحدد هذه المعلمة مدة صلاحية شهادة المرجع المصدق. يمكن تحديد قيمة هذه المعلمة بالأيام/الساعات/الدقائق.

> **ملاحظة**: بالنسبة للأمثلة الواردة في هذا المستند، تبلغ قيمة هذه المعلمة *30 دقيقة*.

شهادة العمر الافتراضي

تحدد هذه المعلمة مدة صلاحية شهادة الهوية التي يتم إصدارها بواسطة موجه CA. يمكن تحديد قيمة هذه المعلمة بالأيام/الساعات/الدقائق.

ملاحظة: بالنسبة للأمثلة الواردة في هذا المستند، تبلغ قيمة هذه المعلمة *20 دقيقة*

التكوين

ملاحظة: يتم إستخدام قيم مؤقت PKI الأصغر *مدى الحياة* و*إعادة التوجيه التلقائي* و*التسجيل التلقائي* **في هذا المستند لتوضيح مفاهيم التسجيل التلقائي الأساسية وإعادة التوجيه التلقائي.** في بيئة شبكة مباشرة، توصي Cisco باستخدام فترات الحياة الافتراضية لهذه المعلمات.

تلميح: يمكن أن تتأثر جميع الأحداث المستندة إلى مؤقت PKI، مثل *إعادة التوجيه* و*إعادة التسجيل*، إذا لم يكن هناك مصدر وقت موثوق. لهذا السبب، توصي Cisco بتكوين بروتوكول وقت الشبكة (NTP) على جميع الموجهات التي تشكل PKI.

تكوين خادم Cisco IOS CA

يقدم هذا القسم مثالا لتكوين خادم 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

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:
```

ملاحظة: القيمة التي يتم تحديدها باستخدام الأمر **auto-over هي عدد الأيام/الساعات/الدقائق** *قبل تاريخ انتهاء صلاحية شهادة CA الحالية* التي يتم إنشاء شهادة المرور الفوقي. لذلك، إذا كانت شهادة CA صالحة من 12:00 إلى 12:30، فإن **التمرير التلقائي 0 0 10** يشير إلى أن شهادة CA المنقولة يتم إنشاؤها حوالي 12:20.

أدخل الأمر **show crypto pki certificate** للتحقق من التكوين على خادم 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
```

استنادا إلى هذا الإخراج، يتضمن الموجه شهادة CA الحالحة من 9:16 إلى 9:46 IST في 25 نوفمبر 2012. ونظرا لأنه تم تكوين المؤقت الالتقاطي لمدة 10 دقائق، فمن المتوقع إنشاء شهادة الظل/المرور الفوقي بحلول *9.36* نوفمبر 25، 2012.

in order to تأكدت، **تقوُم crypto pki العرض** أمر:

```
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
```

استنادا إلى هذا الإخراج، تم إصدار الأمر **show crypto pki timer** في 9.19 IST، ومن المتوقع إنشاء شهادة الظل/المرور في غضون 16.43 دقيقة:

[09:19:22 + 00:16:43] = **09:36:05**، وهو [end-date_of_current_ca_cert - auto_rollover_timer]، أي [09:46:05 - 00:10:00] = **09:36:05**.

تكوين الموجه الذي يتحدث عنه العميل

يقدم هذا القسم الاثم لتكوين موجه العميل/المتحدث.

```
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
```

> **ملاحظة**: يتيح أمر **التسجيل التلقائي** ميزة التسجيل التلقائي على الموجه. صياغة الأمر هي: **التسجيل التلقائي** [*val%*] [*regenerate*].

في الإخراج السابق، يتم تحديد ميزة التسجيل التلقائي على أنها 70%، أي عند نسبة 70% من **[عمر** current_ID_CERT]، يقوم الموجه تلقائيا بإعادة التسجيل مع CA.

> **تلميح**: توصي Cisco بتعيين قيمة التسجيل التلقائي إلى 60% أو أكثر لضمان عمل مؤقتات PKI بشكل صحيح.

يؤدي خيار *إعادة الإنشاء* إلى إنشاء مفتاح Rivest-Shamir-Addleman (RSA) جديد لأغراض إعادة تسجيل/تجديد الشهادة. إذا لم يتم تحديد هذا الخيار، يتم إستخدام مفتاح RSA الحالي.

التسجيل التلقائي في العمل

أكمل الخطوات التالية للتحقق من ميزة التسجيل التلقائي:

1. أدخل الأمر **crypto pki authenticate** من أجل المصادقة يدويا على نقطة الثقة على موجه العميل:

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

ملاحظة: للحصول على مزيد من المعلومات حول هذا الأمر، ارجع إلى مرجع أمر أمان Cisco IOS. بمجرد إدخال الأمر، يجب أن تظهر مخرجات مماثلة لهذا:

```
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. اكتب **نعم** لقبول شهادة CA على موجه العميل. بعد ذلك، يبدأ مؤقت **التجديد** في الموجه:

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

3. بمجرد وصول مؤقت **التجديد** إلى صفر، يقوم موجه العميل بتسجيل نفسه تلقائيا مع المرجع المصدق للحصول على شهادة الهوية الخاصة به. بمجرد إستلام الشهادة، أدخل الأمر **show crypto pki certificate** لعرضها:

```
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
```

تاريخ التجديد وه **09:30:08** ويتم حساب كما وه موضح هنا:

وقت البدء + (٪تجديد ID_CERT_LIFETIME)

وأ

09:16:57 + (70٪ * 20 دقيقة) = **09:30:08**

تعكس أجهزة توقيت PKI نفس الشيء:

```
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. بمجرد انتهاء صلاحية مؤقت **التجديد**، يتم إعادة تسجيل الموجه مع CA للحصول على شهادة معرف جديدة. بعد إجراء تجديد الشهادة، أدخل الأمر **show crypto pki** cert لعرض شهادة المعرف الجديدة:

```
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
```

لاحظ أنه لم يعد هناك *تاريخ تجديد*، بدلا من ذلك، تبدأ مؤقت **الظل**:

```
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
```

وفيما يلي منطق العملية:

- إذا كان تاريخ انتهاء شهادة المعرف **الرسمي** تاريخ انتهاء شهادة CA، **فقم بحساب تاريخ التجديد استنادا إلى النسبة المئوية للتسجيل التلقائي وأبدأ مؤقت التجديد.**

- إذا كان تاريخ انتهاء شهادة **المعرف المساعد** لتاريخ انتهاء شهادة CA، فلا يلزم إجراء عملية تجديد لأن شهادة المعرف الحالية صالحة فقط طالما كانت شهادة CA الحالية صالحة. بدلا من ذلك، تم بدء تشغيل مؤقت **الظل**.

يتم حساب وحدة التوقيت هذه أيضا استنادا إلى النسبة المئوية المذكورة في أمر **التسجيل التلقائي**. على سبيل المثال، ضع في حسابك تواريخ صلاحية شهادة المعرف المتجددة الموضحة في المثال السابق:

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

مدة صلاحية هذه الشهادة هي 16 دقيقة. لذلك، مؤقت المرور الفوقي (أي مؤقت الظل) هو 70٪ من 16 دقيقة، وهو ما يعادل 11 دقيقة تقريبا. يوضح هذا الحساب أن المواجهة يجب أن تطلب الشهادات الظل/المرور الخاصة به في [09:30:09 + 00:11:00] = 09:41:09، والتي تتطابق مع مؤقت ظل PKI الظاهر سابقا في هذا المستند:

```
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
```

التبديل التلقائي قيد التشغيل

يصف هذا القسم الـ mise à niveau سمة في عملية.

على خادم Cisco IOS CA

عندما تنتهي صلاحية مؤقت الظل، تظهر شهادة المرور الفوقي على موجه 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
```

في موجه العميل

كما هو موضح مسبقا في هذا المستند، بدأت ميزة التسجيل التلقائي مؤقت ظل على موجه العميل. عندما تنتهي صلاحية مؤقت الظل، تتيح ميزة التسجيل التلقائي للموجه طلب شهادة *إعادة توجيه/ظل CA*. وبمجرد تلقيها، فإنها تستعلم عن شهادة *إعادة* خادم CA لـ *الظل الخاصة بها* أيضا. ونتيجة لذلك، يحتوي الموجه على زوجين من *التوجيه/معرف*

الشهادات: زوج واحد يكون حاليا والأزواج الأخرى التي تحتوي على شهادات المرور/الظل:

```
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
```

الحظ صلاحية شهادة معرف المرور:

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

تكون مدة صلاحية الشهادة أربع دقائق فقط (بدلا من 20 دقيقة الموقوعة، كما هو مكون على خادم Cisco IOS CA). وفقا لخادم Cisco IOS CA، يجب أن تكون مدة صلاحية شهادة المعرف *للطلب* 20 دقيقة (مما يعني، بالنسبة لموجه عميل محدد، أن مجموع مدد صلاحية شهادات المعرف (الحالية + الظل) الصادرة له يجب ألا يزيد عن 20 دقيقة).

ويرد وصف آخر لهذه العملية هنا:

- فيما يلي صحة شهادة المعرف الحالية على الموجه:

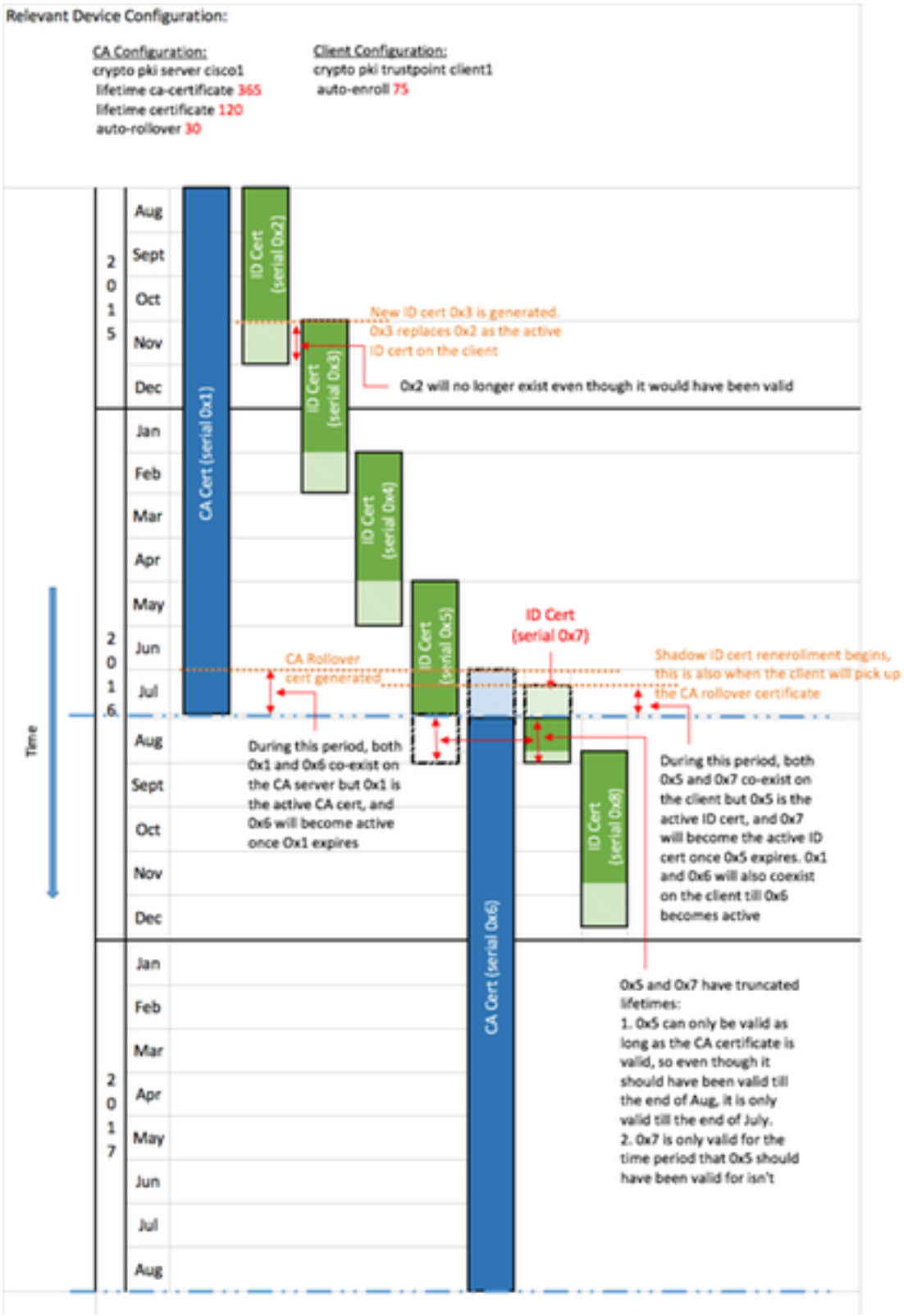
  ```
  start date: 09:30:09 IST Nov 25 2012
  end date: 09:46:05 IST Nov 25 2012
  ```

  لذلك، يكون *current_id_cert_lifetime* 16 دقيقة.
- فيما يلي صحة شهادة معرف المرور:

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

  لذلك، فإن *rollover_id_cert_lifetime* هو أربع دقائق.
- وفقا لبرنامج Cisco IOS، عند إضافة [current_id_cert_lifetime] إلى [rollover_id_cert_lifetime]، يجب أن يساوي [total_id_cert_lifetime]. وهذا صحيح في هذا المثيل.

نموذج لمخطط PKI مع المرور والتسجيل



اعتبارات هامة

- تتطلب وحدات توقيت PKI ساعة موثوقة من أجل العمل بشكل صحيح. توصي Cisco باستخدام NTP لمزامنة الساعات بين موجهات العميل وموجه Cisco IOS CA. في غياب بروتوكول وقت الشبكة (NTP)، يمكن إستخدام ساعة النظام/الأجهزة على الموجه. لمزيد من المعلومات حول كيفية تكوين ساعة الأجهزة وجعلها موثوقة، ارجع إلى دليل تكوين إدارة النظام الأساسية، الإصدار 12.4T من Cisco IOS.

- عند إعادة تحميل الموجه، غالبا ما تستغرق مزامنة بروتوكول وقت الشبكة (NTP) بضع

دقائق. ومع ذلك، يتم إنشاء وحدات توقيت PKI على الفور تقريبا. اعتبارا من الإصداريين 15.2(4)S و 15.2(3.8)T، يتم إعادة تقييم وحدات توقيت PKI تلقائيا بعد مزامنة NTP.

- وحدات توقيت PKI ليست مطلقة، وتعتمد على *الوقت المتبقي*، وبالتالي، تتم إعادة حسابها بعد إعادة التشغيل. على سبيل المثال، افترض أن موجه العميل لديه شهادة معرف صالحة لمدة 100 يوم، وتم تعيين ميزة التسجيل التلقائي على 80٪. بعد ذلك، من المتوقع أن تحدث إعادة التسجيل بعد اليوم الثمانين. إذا تم إعادة تحميل الموجه في اليوم 60، فإنه يبدأ في تمهيد مؤقت PKI وإعادة حسابه كما هو موضح هنا: (*الوقت المتبقي*) * (*التسجيل التلقائي٪*) = (100-60) * 80٪ = 32 يوما.

  لذلك، تتم إعادة التسجيل في اليوم [60+32] = 92.

- عندما تقوم بتكوين التسجيل التلقائي ومؤثرات العدسة التلقائية، فمن المهم تكوينها بقيم تسمح بتوافر شهادة مرجع الظل (CA) على خادم PKI عندما يطلب عميل PKI ذلك. ويساعد هذا على تخفيف حالات التعطل المحتملة لخدمات PKI في بيئة واسعة النطاق.

معلومات ذات صلة

- نشر أمان Cisco IOS باستخدام التقرير الرسمي للبنية الأساسية للمفتاح العام
- البنية الأساسية للمفتاح العام: التقرير الرسمي لمزايا النشر ومميزات النشر
- دليل تكوين البنية الأساسية للمفتاح العام
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).