Contenu

Introduction

Ce document décrit une situation de panne avec un déploiement d'Infrastructure à clés publiques (PKI) de serveur de certificat de Cisco IOS® de large échelle et sa réduction potentielle en accordant correctement les configurations d'event timer de PKI.

Problème

Symptômes d'utilisateur

Ce problème peut être vu dans un environnement de grande puissance de PKI où une autorité d'enregistrement de Cisco IOS (RA) est configurée pour entretenir des centaines et parfois des milliers de périphériques de client de PKI. Quand cette panne particulière se produit, l'inscription de certificat des clients de PKI pourrait échouer par intermittence ou uniformément.

Sur les clients de PKI il est probable que ces messages de log pourraient être vus :

Après que vous activiez ces le PKI met au point :

on le voit que le client demande le certificat inversé de serveur d'Autorité de certification (CA), mais reçoit à la place un message d'erreur non trouvé du « HTTP 404 » du serveur CA.

```
Dec 31 03:14:19.184: PKI: Shadow state for GETVPN now
GET_NEW_CA_CERT_WAIT_FOR_RETRY
Dec 31 03:14:19.184: PKI:get_cert GETVPN 0x10 (expired=0):
Dec 31 03:14:19.184: PKI: Shadow state for GETVPN now GET_NEW_CA_CERT
Dec 31 03:14:39.187: PKI: Shadow timer went off for GETVPN
Dec 31 03:14:39.187: CRYPTO_PKI: Sending Next CA Certificate Request:
GET /cgi-bin/pkiclient.exe?operation=GetNextCACert&message=GETVPN HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
Host: 192.168.105.3


Dec 31 03:14:39.187: CRYPTO_PKI: locked trustpoint GETVPN, refcount is 1
```

```
Dec 31 03:14:39.187: CRYPTO_PKI: http connection opened
Dec 31 03:14:39.187: CRYPTO_PKI: Sending HTTP message

Dec 31 03:14:39.191: CRYPTO_PKI: Reply HTTP header:
HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
Host: 192.168.105.3


Dec 31 03:14:39.203: CRYPTO_PKI: unlocked trustpoint GETVPN, refcount is 0
Dec 31 03:14:39.203: CRYPTO_PKI: locked trustpoint GETVPN, refcount is 1
Dec 31 03:14:39.223: CRYPTO_PKI: unlocked trustpoint GETVPN, refcount is 0
Dec 31 03:14:39.223: CRYPTO_PKI: Reply HTTP header:
HTTP/1.1 404 Not Found
Date: Tue, 30 Dec 2014 16:14:28 GMT
Server: cisco-IOS
Accept-Ranges: none

Content-Type indicates we did not receive a certificate.

Dec 31 03:14:39.227: %Error in connection to Certificate Authority:
status = FAIL
```

> Remarque: Cette question n'est pas particularité de RA et peut également se produire quand un RA n'est pas utilisé (CA seulement).

Dépannez et identification de problème

Un des symptômes principaux observés dans la panne est qu'il y a beaucoup de demandes de PKI sur le ce de RA provenu les clients de PKI. Ceci peut être vu avec des sorties de capture de NetFlow ou de paquet. La quantité de demandes de PKI peut accabler le serveur de sorte qu'elle ne puisse pas répondre assez rapidement. Une manière de vérifier cette condition est au telnet au serveur CA sur le port HTTP qu'elle écoute. Quand le service écoute sur le port et répond, vous devriez voir la connexion ouverte. Dans l'état défaillant, la tentative de telnet chronomètre qui indique que le TCP ne termine pas même la prise de contact à trois voies.

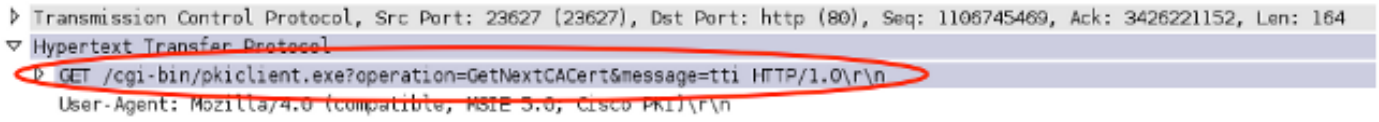
Afin de comprendre mieux pourquoi le TCP échoue, sélectionnez la commande de **<tcp_peer_address> d'adresse de transactions de TCP d'IP de débogage** sur le serveur afin de gagner des vues dans la manipulation du serveur des écoulements de TCP à une adresse source particulière de TCP (il est important de spécifier le filtre d'adresse quand vous mettez au point un environnement de grande puissance). Dans l'état défaillant, ceux-ci met au point sont observés :

```
Dec 31 03:14:19.184: PKI: Shadow state for GETVPN now
GET_NEW_CA_CERT_WAIT_FOR_RETRY
Dec 31 03:14:19.184: PKI:get_cert GETVPN 0x10 (expired=0):
Dec 31 03:14:19.184: PKI: Shadow state for GETVPN now GET_NEW_CA_CERT
Dec 31 03:14:39.187: PKI: Shadow timer went off for GETVPN
Dec 31 03:14:39.187: CRYPTO_PKI: Sending Next CA Certificate Request:
GET /cgi-bin/pkiclient.exe?operation=GetNextCACert&message=GETVPN HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
Host: 192.168.105.3
```

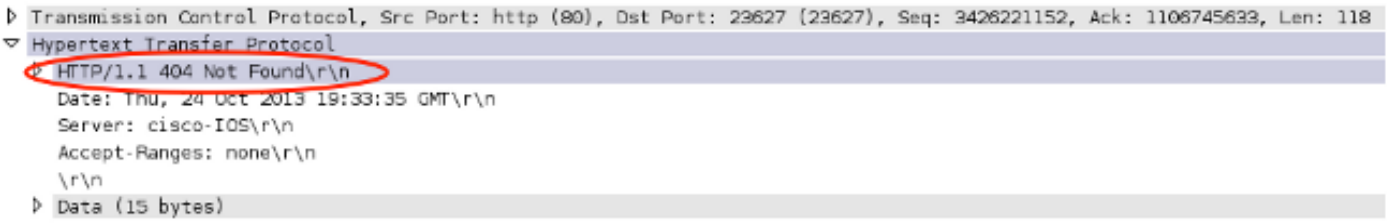
```
Dec 31 03:14:39.187: CRYPTO_PKI: locked trustpoint GETVPN, refcount is 1
Dec 31 03:14:39.187: CRYPTO_PKI: http connection opened
Dec 31 03:14:39.187: CRYPTO_PKI: Sending HTTP message

Dec 31 03:14:39.191: CRYPTO_PKI: Reply HTTP header:
HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
Host: 192.168.105.3


Dec 31 03:14:39.203: CRYPTO_PKI: unlocked trustpoint GETVPN, refcount is 0
Dec 31 03:14:39.203: CRYPTO_PKI: locked trustpoint GETVPN, refcount is 1
Dec 31 03:14:39.223: CRYPTO_PKI: unlocked trustpoint GETVPN, refcount is 0
Dec 31 03:14:39.223: CRYPTO_PKI: Reply HTTP header:
HTTP/1.1 404 Not Found
Date: Tue, 30 Dec 2014 16:14:28 GMT
Server: cisco-IOS
Accept-Ranges: none

Content-Type indicates we did not receive a certificate.

Dec 31 03:14:39.227: %Error in connection to Certificate Authority:
status = FAIL
```

> **Conseil** : Dans les versions 15.1 et 15.2 la commande de **transactions de TCP d'IP de débogage** n'a pas une option d'adresse là-dessus. Au lieu de cette commande, écrivez les **<tcp_peer_address d'adresse de paquet de TCP d'IP de débogage** afin d'afficher également si la limite de file d'attente de connexion est atteinte.

Une capture de paquet pour les demandes de PKI peut également aider à indiquer les informations complémentaires au sujet de ce que sont ces demandes de PKI. De la capture de paquet, vous pouvez voir un grand nombre de requêtes semblable à :



Pour certaines de ces demandes aux lesquelles le serveur peut réellement répondre, vous voyez également un "404 ne pas fonder la » réponse :



Cause principale

Il y a quelques facteurs qui contribuent à ce problème particulier. D'abord, le GetNextCACert prouve que ces demandes de PKI sont des demandes inversées des clients de demander pour un renversement/certificat de CA de shadow. Pour plus de détails sur l'exécution inversée CA, voir l' auto-enroll, l'auto-rollover, et les temporisateurs de PKI IOS. La » réponse "404 non trouvée indique que le serveur RA/CA ne pourrait pas avoir le certificat de shadow au moment de la demande. Ceci peut être vérifié avec la **crypto** sortie de commande de **certificat de PKI d'exposition** sur les serveurs CA et de RA. Le problème est dû à cette configuration de temporisateur de certificat trouvée sur le serveur et le client de PKI :

Serveur RA/CA

```
CA-Server#show running | section pki server
crypto pki server ca-server
<snip>
lifetime certificate 600
lifetime ca-certificate 1825
auto-rolloverCA-Server#show crypto pki server | include Rollover
Auto-Rollover configured, overlap period 30 days
CA-Server#
```

Clients de PKI

```
crypto pki trustpoint test enroll url http://enrollment_url.test.com:80
enrollment mode ra subject-name OU = TEST OU, OU = cisco auto-enroll 70
```

Le problème est que l'heure de validité de certificat de CA est configurée d'être de 5 ans (1825 jours), mais le renversement/certificat de shadow n'obtient pas créé sur le serveur CA jusqu'à 30 jours avant l'échéance de certificat valable. Les Certificats de routeur ont un temps de validité de 600 jours, et basé sur la configuration d'auto-enroll, le routeur pourrait demander un renversement/certificat de shadow après 70% de la vie de 600 jours. Ceci a pu avoir lieu dès 180 jours avant le temps d'expiration en cours de certificat de CA. Pour un calcul détaillé de ces périodes et l'explication des événements de PKI, référez-vous de nouveau à l'auto-enroll, à l'auto-rollover, et aux temporisateurs de PKI IOS. Ceci explique pourquoi les clients continuent à demander le renversement/shadow CA, et continue à recevoir la » erreur "404 non trouvée puisqu'ils ne sont pas créés sur le serveur encore. Cette condition persiste jusqu'à ce que le renversement CA/certificat de shadow soit généré.

Dans le même temps, en raison d'un grand nombre de demandes qui entrent dans le serveur de RA, le serveur de RA de Cisco IOS peut dépasser ces seuil et début de connexion HTTP pour relâcher des demandes de connexion HTTP entrantes :

- La limite simultanée de connexions au serveur de HTTP maximum. Ceci peut être changé à un maximum de 16 connexions simultanées avec la commande de l'**ip http max-connections 16**.
- La limite interne de vitesse de connexion de serveur HTTP de 80 connexions par minute. Quand ce seuil est atteint, le serveur HTTP de theCiscoIOS étrangle de retour et cesse d'écouter de nouvelles demandes de HTTP pendant 15 secondes. Actuellement, ce seuil de raté limit n'est pas utilisateur configurable. En conséquence, le theTCP erreur « atteinte par limite » de file d'attente de connexion est vu avec la transaction de theTCP met au point.

Remarque: Actuellement le seuil ci-dessus ne peut pas être surveillé avec une

commande Cisco IOS. Une demande d'amélioration a été ouverte d'améliorer ceci, voient l'ID de bogue Cisco CSCuj83430.

Solution

La solution au problème est de corriger les configurations d'event timer de PKI sur le serveur CA tels qu'un renversement/certificat de shadow est généré avant n'importe quelle demande inversée de client de PKI. Ceci peut être fait avec ces étapes :

1. Sélectionnez la **commande shutdown** sous la commande du crypto pki server command.in de désactiver le serveur CA.
2. Augmentez le temps inversé de superposition basé sur la vie de certificat et la configuration de reenrollment :

```
CA-Server(config)#crypto pki server ca-server
CA-Server(cs-server)#auto-rollover ?
<0-1825> Overlap time between CA certificates during rollover, in days
<cr>
CA-Server(cs-server)#auto-rollover 365
```

3. Réactivez le serveur CA.
4. S'il y a anRA, manuellement theRA inversé pour récupérer le renversement/certificat de shadow.

> **Conseil** : Afin de forcer le CA au renversement manuellement sans activer l'auto-rollover, sélectionnez la commande de **renversement de <server-name> de crypto pki server**.

En outre, comme discuté précédemment, il est recommandé pour augmenter la limite maximum de connexion simultanée de HTTP à 16 pour que le serveur manipule une vitesse de connexion entrante élevée.