Contenido

Introducción

Este documento describe una situación de falla con un despliegue del Public Key Infrastructure (PKI) del servidor de certificados del ® del Cisco IOS del gran escala y su mitigación potencial correctamente ajustando las configuraciones del temporizador del evento PKI.

Problema

Síntomas del usuario

Este problema se puede considerar en un entorno en grande PKI donde un registration authority (RA) del Cisco IOS se configura para mantener los centenares y a veces los millares de dispositivos del cliente PKI. Cuando ocurre esta falla determinada, la inscripción del certificado de los clientes PKI pudo fallar intermitentemente o constantemente.

En los clientes PKI es probable que estos mensajes del registro puedan ser considerados:

Después de que usted habilite estos debugs PKI:

se ve que los pedidos de cliente el certificado de la renovación del servidor del Certificate Authority (CA), sino que por el contrario reciben un mensaje de error no encontrado “HTTP 404” del servidor de 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
```

> Nota: Este problema no es RA específico y puede también suceder cuando un RA no se utiliza (CA solamente).

Troubleshooting y Identificación del problema

Uno de los síntomas dominantes observados en el error es que hay muchas peticiones PKI en el RA que vienen de los clientes PKI. Esto se puede ver con las salidas del Netflow o de la captura de paquetes. La cantidad de peticiones PKI puede abrumar el servidor de modo que no pueda responder rápidamente bastante. Una manera de verificar esta condición es al telnet al servidor de CA en el puerto HTTP que está escuchando. Cuando el servicio escucha en el puerto y responde, usted debe ver la conexión abierta. En el estado fallido, la tentativa telnet mide el tiempo hacia fuera que indica que el TCP ni siquiera acaba el apretón de manos de tres vías.

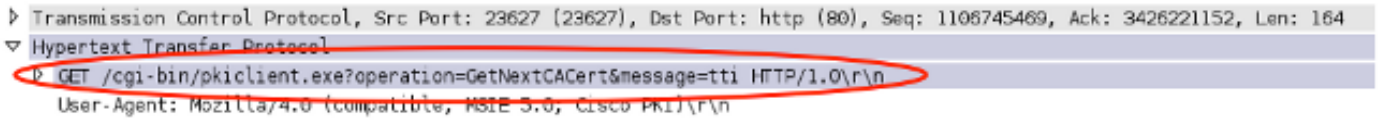
Para entender mejor porqué el TCP falla, ingrese el comando del **<tcp_peer_address> del direccionamiento de las transacciones tcp del IP del debug** en el servidor para ganar las penetraciones en la dirección del servidor de los flujos TCP a una dirección de origen determinada TCP (es importante especificar el filtro de direcciones cuando usted hace el debug de un entorno en grande). En el estado fallido, se observan estos debugs:

```
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)
```

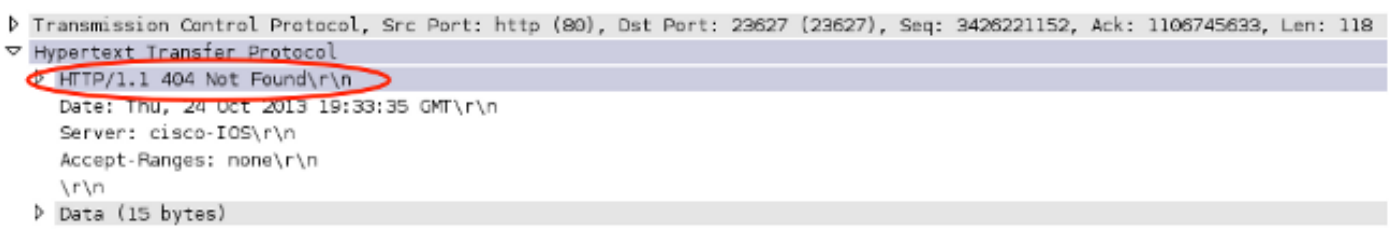
```
Host: 192.168.105.3


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
```

> Consejo: En las versiones 15.1 y 15.2 el **comando debug ip tcp transactions** no tiene una opción de dirección en ella. En lugar de este comando, ingrese los **<tcp_peer_address del direccionamiento del paquete tcp del IP del debug** para también mostrar si se alcanza el límite de la cola de conexión.

Una captura de paquetes para las peticiones PKI puede también ayudar a revelar la información adicional sobre cuáles son estas peticiones PKI. De la captura de paquetes, usted puede ver un número grande de peticiones similares a:



Para algunas de estas peticiones que el servidor puede responder realmente a, usted también ve un "404 no encontrar la" respuesta:



Causa raíz

Hay algunos factores que contribuyen a este problema determinado. Primero, el GetNextCACert muestra que estas peticiones PKI son peticiones de la renovación de los clientes de petición una renovación/el certificado de CA de la sombra. Para más detalles en la operación de la renovación de CA, vea IOS PKI Auto-alistar, Auto-renovación, y temporizadores. La" respuesta no encontrada "404 indica que el servidor RA/CA no pudo tener el certificado de la sombra a la hora de la petición. Esto se puede verificar con el **comando certificate crypto del pki de la demostración** hecho salir en los servidores de CA y RA. El problema es debido a esta configuración del temporizador del certificado encontrada en el servidor pki y el cliente:

Servidor 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#
```

Clientes 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
```

El problema es que la época de la validez del certificado de CA está configurada de ser 5 años (1825 días), pero la renovación/el certificado de la sombra no consigue creados en el servidor de CA hasta 30 días antes del vencimiento actual del certificado. Los certificados del router tienen un rato de la validez de 600 días, y basado en la configuración del auto-alistar, el router podría pedir una renovación/un certificado de la sombra después del 70% del curso de la vida de 600 días. Esto podía ser ya desde 180 días antes del vencimiento actual del certificado de CA. Para un cálculo detallado de estas épocas y la explicación de los eventos PKI, refiera otra vez a IOS PKI Auto-alistan, Auto-renovación, y los temporizadores. Esto explica porqué los clientes continúan pidiendo la renovación/la sombra de CA, y continúa recibiendo el" error no encontrado "404 puesto que no se crean en el servidor todavía. Esta condición persiste hasta que se genere la renovación de CA/el certificado de la sombra.

Mientras tanto, debido a una gran cantidad de las peticiones que entran en el servidor RA, el servidor del Cisco IOS RA puede exceder este umbral de la conexión HTTP y comenzar a caer las peticiones de conexión HTTP entrantes:

- El límite simultáneo de las conexiones del servidor del máximo HTTP. Esto se puede cambiar a un máximo de 16 conexiones concurrentes con **ip http el** comando de las MAX-**conexiones 16**.
- El límite interno de la velocidad de conexión del servidor HTTP de 80 conexiones por el minuto. Cuando se alcanza este umbral, el servidor HTTP del theCiscoIOS estrangula detrás y para el escuchar los nuevos pedidos de HTTP por 15 segundos. Actualmente, este umbral del límite de velocidad no es usuario configurable. Como consecuencia, el theTCP error alcanzado límite de la "cola de conexión" se considera con los debugs de la transacción del

theTCP.

Nota: El umbral antedicho no se puede monitorear actualmente con un comando cisco ios. Se ha abierto un pedido de mejora de mejorar esto, considera el Id. de bug Cisco CSCuj83430.

Solución

La solución a este problema es corregir las configuraciones del temporizador del evento PKI en el servidor de CA tales que una renovación/un certificado de la sombra está generada antes de cualquier petición de la renovación del cliente PKI. Esto se puede hacer con estos pasos:

1. Ingrese el **comando shutdown** bajo pedido crypto del servidor pki command.in de inhabilitar el servidor CA.
2. Aumente el tiempo de la coincidencia de la renovación basado en el curso de la vida del certificado y la configuración del 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. Vuelva a permitir el servidor de CA.
4. Si hay anRA, theRA de la renovación para extraer manualmente la renovación/el certificado de la sombra.

Consejo: Para forzar el CA a la renovación manualmente sin habilitar la auto-renovación, ingrese el comando **crypto de la renovación del servidor pki <server name>**.

También, según lo discutido previamente, se recomienda para aumentar el límite máximo de la conexión concurrente HTTP a 16 para que el servidor maneje una alta tarifa de la conexión entrante.