Problemas de integración de Prime Infrastructure 3.5+ debido al certificado TOFU

Contenido

Introducción

Este documento describe el problema de integración que se produce debido a la discordancia del certificado de confianza en el primer uso (TOFU) después de que se genere una nueva solicitud de firma de certificado (CSR) en Cisco Prime Infrastructure (primaria/secundaria), cómo resolver problemas y resolverlo.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Infraestructura Cisco Prime
- Alta disponibilidad

Componentes Utilizados

La información que contiene este documento se basa en la versión 3.5 y posteriores de Cisco Prime Infrastructure.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red

en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Estos son los documentos de referencia que proporcionan información sobre alta disponibilidad y generación de certificados en Cisco Prime Infrastructure.

Guía de alta disponibilidad: https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-6/admin/guide/bk_CiscoPrimeInfrastructure_3_6_AdminGuide/bk_CiscoPrimeInfrastructure_3_6_AdminGuide_chapter_01011.html

Guía del administrador: https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-6/admin/guide/bk_CiscoPrimeInfrastructure_3_6_AdminGuide/bk_CiscoPrimeInfrastructure_3_6_AdminGuide_chapter_0100.html

Problema

TOFU - El certificado recibido del host remoto es de confianza cuando la conexión se realiza por primera vez.

El certificado TOFU en la infraestructura principal o el host remoto al que se conecta prime puede cambiar si se genera un nuevo certificado o si el servidor se implementa de nuevo en el host VM.

La generación e importación de un nuevo CSR en el servidor de infraestructura principal (principal/secundario) envía la nueva información de certificado TOFU a los servidores remotos cuando se reinicia la conectividad después de un reinicio del servicio.

Si el host remoto envía un certificado diferente para cualquier conexión subsecuente después de la primera, la conexión será rechazada.

El host remoto podría ser (servidor primario o secundario en la implementación de HA, servidor de motor de servicio integrado (ISE)) donde el antiguo TOFU todavía está presente.

Esto provoca una falla de registro entre los servidores primario y secundario, Prime y el servidor ISE.

La sección Troubleshooting describe los mensajes de error que se pueden encontrar en los registros del monitor de estado en tales escenarios.

Troubleshoot

En el registro del monitor de estado primario, se pueden encontrar estos mensajes de error que señalan la discordancia en el certificado secundario.

```
[system] [HealthMonitorThread] TOFU failed.
Check local trust Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
- CN=prime-sec, OU=Prime Infra, O=Cisco Systems, L=SJ, ST=CA, C=US
```

```
javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException:
Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
- CN=prime-sec
```

Estos mensajes de error se pueden encontrar en los registros de la infraestructura principal que señalan la discordancia en el certificado del servidor ISE.

```
[system] [seqtaskexecutor-3069] TOFU failed.
Check local trust Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
- CN=ISE-server

javax.net.ssl.SSLHandshakeException: java.security.cert.
CertificateException: Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
- CN=ISE-server
```

En el registro del monitor de estado secundario, se pueden encontrar estos mensajes de error que señalan la discordancia en el certificado primario.

```
[system] [HealthMonitorThread] TOFU failed.
Check local trust Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
- CN=prime-pri, OU=Prime Infra, O=Cisco Systems, L=SJ, ST=CA, C=US


javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException:
Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
- CN=prime-pri
```

Solución

Es necesario enumerar los certificados TOFU actuales en prime, de ahí que la antigua entrada de certificado para el host remoto correspondiente se identifique y elimine antes de intentar la integración de primo de nuevo.

Configuración

Ver lista de validación de certificados

El comando **ncs certValidation tofu-certs listcerts** se puede utilizar para ver la lista de validación de certificados.

Este resultado proviene del servidor principal de Cisco Prime Infrastructure [IP=1XX.XX.XX.XX]:

```
prime-pri/admin# ncs certvalidation tofu-certs listcerts

Host certificate are automatically added to this list on first connection,
if trust-on-first-use is configured - ncs certvalidation certificate-check ...

host=1X.XX.XX.XX_8082;  subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=prime-pri
host=1Z.ZZ.ZZ.ZZ_443;  subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=ISE-server
```

```
host=1YY.YY.YY.YY_8082;  subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=prime-sec

prime-pri/admin#
```

Este resultado proviene del servidor secundario Cisco Prime Infrastructure [IP=1YY.YY.YY.YY]

```
prime-sec/admin# ncs certvalidation tofu-certs listcerts

Host certificate are automatically added to this list on first connection,
if trust-on-first-use is configured - ncs certvalidation certificate-check ...

host=1YY.YY.YY.YY_8082;  subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=prime-sec
host=127.0.0.1_8082;  subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=prime-sec
host=1X.XX.XX.XX_8082; subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=prime-pri

prime-sec/admin#
```

Eliminar certificado

Utilice el comando **ncs certValidation tofu-certs deletecert host <host>** para eliminar a la validación de certificados.

Desde el servidor primario, verifique y elimine las entradas antiguas para los certificados de ISE y TOFU del servidor secundario respectivamente.

- **ncs certValidation tofu-certs deletecert host** 1YY.YY.YY.YY_8082
- **ncs certValidation tofu-certs deletecert host** 1Z.ZZ.ZZ.ZZ_443

Desde el servidor secundario, verifique y elimine las entradas antiguas para el certificado tofu del servidor primario con el uso del comando **ncs certValidation tofu-certs delete erecert host** 1X.XX.XX.XX_8082.

Reinicializar HA de primario a secundario

Paso 1. Inicie sesión en Cisco Prime Infrastructure con una ID de usuario y una contraseña que tengan privilegios de administrador.

Paso 2. En el menú, vaya a **Administration > Settings > High Availability**. Cisco Prime Infrastructure muestra la página de estado de HA.

Paso 3. Seleccione HA Configuration y, a continuación, complete los campos de la siguiente manera:

1. Servidor secundario: Introduzca la dirección IP o el nombre de host del servidor secundario.
2. Clave de autenticación: Introduzca la contraseña de la clave de autenticación que ha establecido durante la instalación del servidor secundario.
3. Dirección de correo electrónico: Introduzca la dirección (o lista de direcciones separada por comas) a la que se debe enviar la notificación sobre los cambios de estado de HA. Si ya ha configurado las notificaciones de correo electrónico mediante la página Configuración del servidor de correo (consulte "Configuración de los parámetros del servidor de correo electrónico"), las direcciones de correo electrónico que introduzca aquí se agregarán a la lista de direcciones ya configuradas para el servidor de correo.
4. Tipo de conmutación por fallo: Seleccione Manual (Manual) o Automatic (Automático). Se recomienda seleccionar Manual.

Se recomienda utilizar el servidor DNS para resolver el nombre de host a una dirección IP. Si utiliza el archivo **/etc/hosts** en lugar del servidor DNS, debe introducir la dirección IP secundaria en lugar del nombre de host.

Paso 4. Si utiliza la función IP virtual, seleccione la casilla de verificación **Enable Virtual IP** (Habilitar IP virtual) y, a continuación, complete los campos adicionales de la siguiente manera:

1. IP virtual IPV4: Introduzca la dirección IPv4 virtual que desea que utilicen ambos servidores HA.
2. IP virtual IPV6: (Opcional) Introduzca la dirección IPv6 que desea que utilicen ambos servidores HA.

El direccionamiento IP virtual no funcionará a menos que ambos servidores estén en la misma subred. No debe utilizar el bloque de direcciones IPV6 fe80, se ha reservado para el direccionamiento de unidifusión local de link.

Paso 5. Haga clic en **Verificar preparación** para asegurarse de que los parámetros ambientales relacionados con HA están listos para la configuración.

Paso 6. Haga clic en **Register** para ver la barra de progreso Milestone, para verificar la finalización del 100% del registro Pre-HA, la replicación de la base de datos y el registro Post HA, como se muestra aquí. Cisco Prime Infrastructure inicia el proceso de registro de HA. Cuando el registro se complete correctamente, el **Modo de configuración** mostrará el valor de Activo primario.

Reconfigurar servidores ISE

Paso 1. Vaya a **Administración > Servidores > Servidores ISE**

Paso 2. Vaya a **Select a command > Add ISE Server** y, a continuación, haga clic en **Ir**
Paso 3. Introduzca la dirección IP, el nombre de usuario y la contraseña del servidor ISE

Paso 4. Confirme la contraseña del servidor ISE.

Paso 5. Click **Save**.

Verificación

El comando **ncs certValidation tofu-certs listcerts** se puede utilizar para verificar el nuevo certificado.

Información Relacionada

- Notas de la versión de Cisco Prime Infrastructure: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-release-notes-list.html
- Guía de inicio rápido de Cisco Prime Infrastructure: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-installation-guides-list.html
- Guía de Referencia de Comandos de Cisco Prime Infrastructure: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-command-reference-list.html
- Guía del usuario de Cisco Prime Infrastructure: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html
- Guía del administrador de Cisco Prime Infrastructure: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-maintenance-guides-list.html
- **Soporte Técnico y Documentación - Cisco Systems**