Resolución de problemas de licencias en Nexus 9000

Contenido

Introducción

En este documento se describen los tipos de errores más frecuentes con las licencias inteligentes en los switches Nexus serie 9000.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Licencias inteligentes en el switch Nexus serie 9000
- Cisco Smart License Utility (CSLU)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Errores de falla de comunicaciones

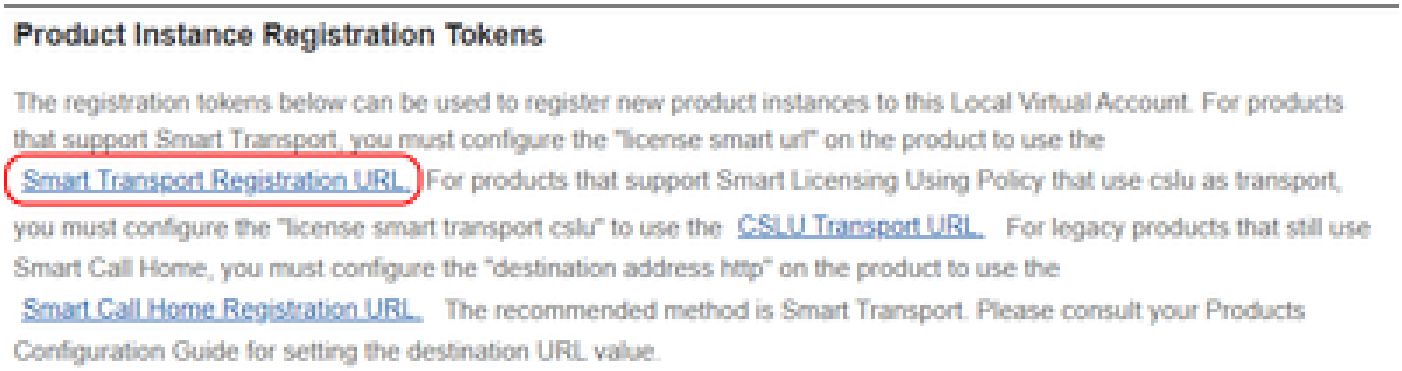
"No se puede establecer una conexión segura porque no se puede validar el certificado TLS del servidor"

Este error de CSLU se produce normalmente por la configuración de un FQDN incorrecto mediante los comandos license smart url cslu o license smart url, o bien por algún dispositivo de la ruta que realiza la suplantación de SSL (normalmente un firewall con la inspección de SSL habilitada).

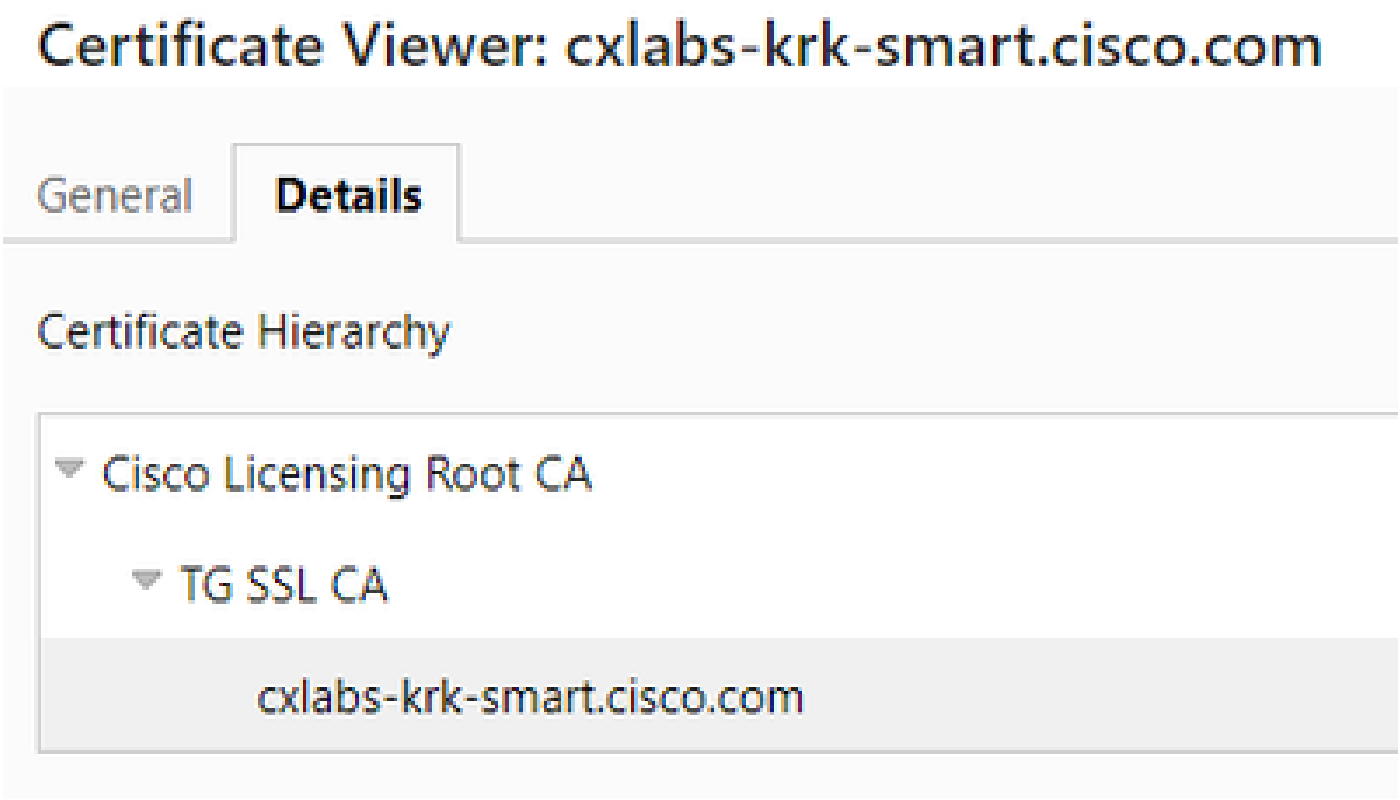
HTTPS en un switch Nexus no es diferente de cualquier sistema operativo cliente típico. Al acceder a un enlace HTTPS, el cliente verificará el FQDN al que está intentando acceder con el FQDN recibido en el certificado, ya sea el campo CN del encabezado de asunto o el campo SAN. El cliente también valida si el certificado recibido está firmado por una entidad emisora de certificados de confianza.

Si intenta acceder a https://www.cisco.com, su navegador lo abrirá sin problemas. Sin embargo, si abre https://173.37.145.84, recibe una advertencia de que no se puede confiar en la conexión, aunque www.cisco.com se resolvería en 173.37.145.84. El explorador está intentando obtener acceso a 173.37.145.84, no ve "173.37.145.84" en el certificado presentado por el servidor, por lo que el certificado no se considera válido.

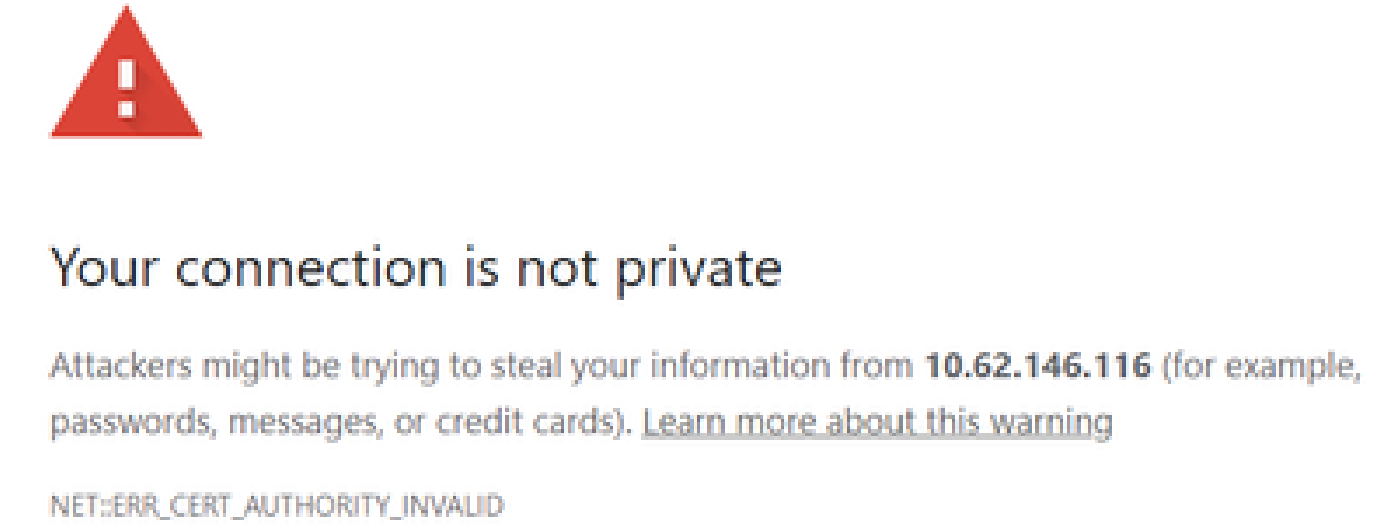
Esta es la razón por la que al configurar la dirección CSSM en el switch, es fundamental utilizar exactamente la URL propuesta por el propio CSSM; contiene el FQDN incrustado en el certificado:



También es importante recordar que hay certificados independientes utilizados para la administración CSSM en las instalaciones (el puerto 8443 es el predeterminado) y el registro de licencias (el puerto 443 es el predeterminado). El certificado de administración puede ser autofirmado o firmado por una CA empresarial local de confianza dentro de la organización o por una CA de confianza global, pero las licencias siempre utilizan una CA raíz de licencias de Cisco especial. Esto se realiza automáticamente sin la intervención adicional del usuario:



Los switches de Cisco confían en esta CA, pero no los PC cliente normales. Si intenta acceder a la URL propuesta por CSSM mediante un PC, el navegador muestra un error debido a que no confía en la CA, pero el switch no tiene ningún problema:



Sin embargo, si hay un firewall que realiza una inspección SSL con suplantación de certificados entre el switch y el servidor CSSM, el firewall sustituye el certificado firmado por la CA de Cisco por un certificado diferente firmado normalmente por una CA empresarial, en la que confían todos los PC y servidores de la organización, pero no el switch. Asegúrese de excluir cualquier tráfico a CSSM de la inspección HTTPS.

Al solucionar el error "El certificado TLS del servidor no se puede validar", acceda a la URL

configurada en el switch con un navegador e inspeccione si el certificado está firmado correctamente por la CA de Cisco y si el FQDN en la cadena de URL coincide con el FQDN en el certificado.

"Fallo de comunicaciones" o "No se pudo resolver el host: cslu-local"

El CSSM suele configurarse con un FQDN en la URL y, en la mayoría de las implementaciones de Nexus, no se configura DNS, lo que suele provocar este tipo de fallos.

El primer paso de la solución de problemas sería hacer ping al FQDN configurado desde el VRF utilizado para Smart Licensing. Por ejemplo, con esta configuración:

```
license smart transport smart
license smart url smart https://smartreceiver.cisco.com/licservice/license
license smart vrf management
```

```
switch# ping smartreceiver.cisco.com vrf management
% Invalid host/interface smartreceiver.cisco.com
```

Este error indica que la resolución DNS en la administración VRF no funciona. Verifique la configuración ip name-server bajo el VRF especificado. Tenga en cuenta que la configuración del servidor DNS es por VRF, por lo que la configuración ip name-server en el VRF predeterminado no tiene efecto en la Administración de VRF. Como solución de interrupción, ip host se puede utilizar para agregar una entrada manual, pero asuma que en el futuro, la dirección IP del servidor puede cambiar y esta entrada puede volverse inválida.

Si el nombre de dominio se resuelve, pero los pings fallan, esto podría ser causado por un firewall que bloquea los pings salientes. En este caso, puede utilizar telnet para probar si el puerto 443 está abierto.

```
switch# telnet smartreceiver.cisco.com 443 vrf management
```

Si esto tampoco funciona, resuelva el problema de la trayectoria de red hacia el servidor y asegúrese de que funcione.

"No se pudo enviar el mensaje HTTP de soporte remoto"

Este mensaje es fundamentalmente similar al mensaje "Fallo de comunicaciones". La diferencia radica en que, por lo general, se ve en switches que ejecutan licencias inteligentes heredadas, no en las licencias inteligentes que utilizan políticas que se introdujeron en la versión 10.2 de NXOS.

Con las licencias inteligentes heredadas, la URL a la que se accede se configura mediante el comando callhome.

```
callhome
...
destination-profile CiscoTAC-1 transport-method http
destination-profile CiscoTAC-1 index 1 http https://tools.cisco.com/its/service/oddce/services/DDCEServ
transport http use-vrf management
```

Asegúrese de que la configuración sea correcta, que utilice HTTPS y que la URL (normalmente tools.cisco.com) esté accesible a través del VRF seleccionado.

Solución de problemas adicional

Consulte Solución de problemas de licencias inteligentes mediante la resolución de problemas de políticas en la solución de Data Center para obtener una lista de comprobación detallada de la resolución de problemas que incluye otros pasos que se pueden realizar para resolver problemas relacionados con las licencias.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).