Licentiefouten opsporen op Nexus 9000

Inhoud

Inleiding

Dit document beschrijft de meest voorkomende soorten fouten met Smart Licensing op Nexus 9000 Series switches.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Smart Licensing op Nexus 9000 Series switch
- Cisco Smart License Utility (CSLU)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Communicatiefouten

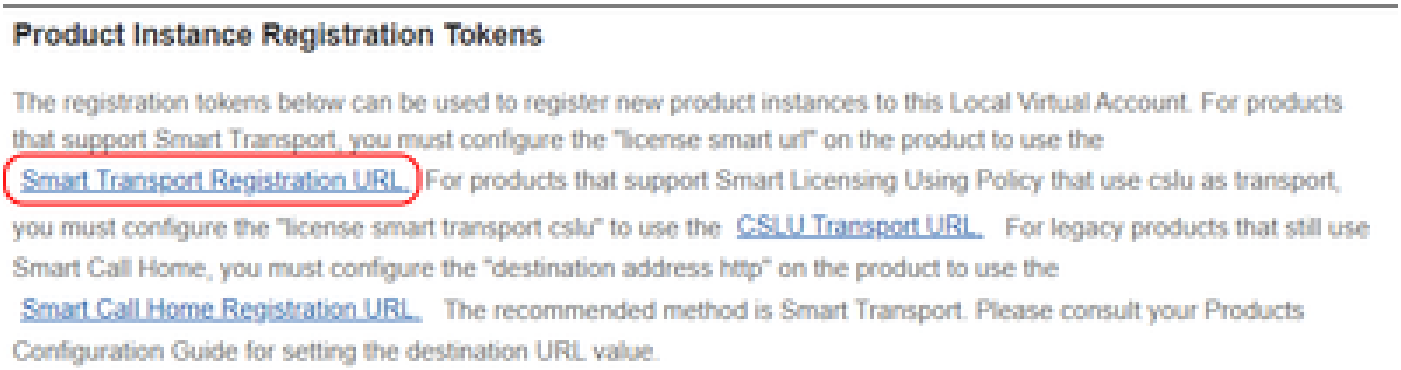
"Kan geen beveiligde verbinding tot stand brengen omdat TLS-beveiliging van server niet kan worden gevalideerd"

Deze CSLU-fout wordt doorgaans veroorzaakt door een onjuiste FQDN te configureren met behulp van de opdrachten smart url cslu of smart url smart, of door een apparaat in het pad dat SSL-spoofing uitvoert (doorgaans een firewall met SSL-inspectie ingeschakeld).

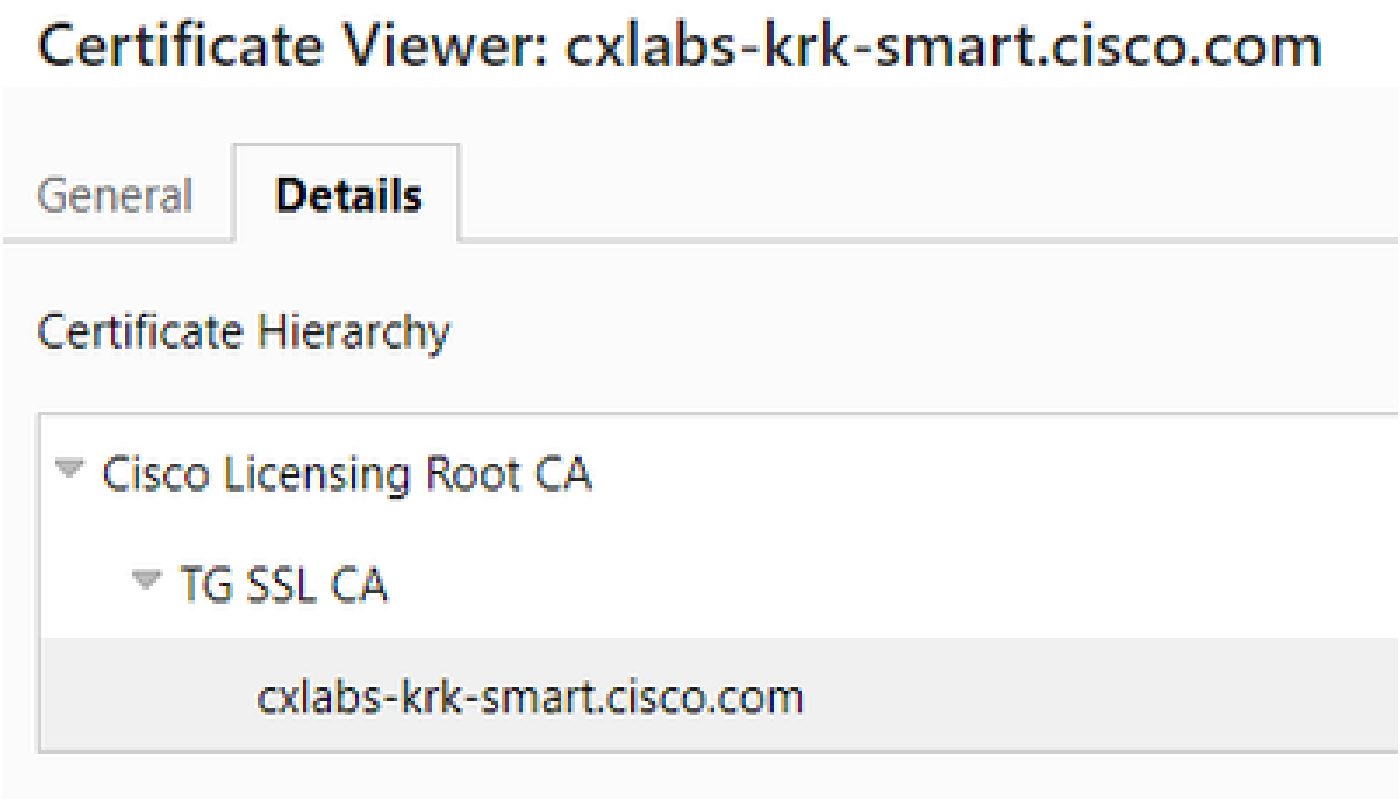
HTTPS op een Nexus switch verschilt niet van alle typische client-OS. Wanneer de client een HTTPS-link opent, zou hij de FQDN die hij probeert te bereiken, verifiëren aan de hand van de FQDN die hij in het certificaat ontvangt - ofwel het veld CN in de kop Onderwerp, ofwel het veld SAN. De klant valideert ook of het ontvangen certificaat is ondertekend door een vertrouwde certificeringsinstantie.

Als u probeert toegang te krijgen tot https://www.cisco.com, opent uw browser het zonder problemen. Echter, als u https://173.37.145.84 opent, krijgt u een waarschuwing dat de verbinding niet kan worden vertrouwd, ook al zou www.cisco.com oplossen naar 173.37.145.84. De browser probeert toegang te krijgen tot 173.37.145.84, het ziet niet "173.37.145.84" in het certificaat gepresenteerd door de server, dus het certificaat wordt niet geldig geacht.

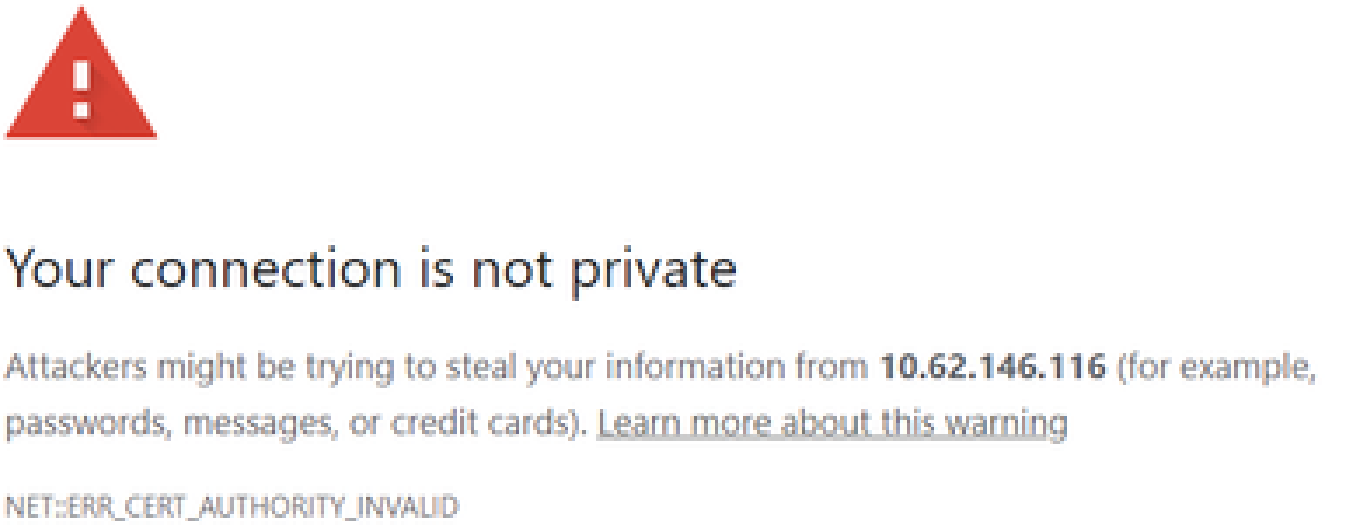
Dit is waarom bij het configureren van het CSSM-adres op de switch, het van cruciaal belang is om exact de URL te gebruiken die door CSSM zelf wordt voorgesteld; het bevat FQDN ingebed in het certificaat:



Het is ook belangrijk om te onthouden dat er afzonderlijke certificaten worden gebruikt voor CSSM On-Prem Management (standaard poort 8443) en licentieregistratie (standaard poort 443). Het beheercertificaat kan zelfondertekend worden of ondertekend worden door een lokale CA die binnen de organisatie wordt vertrouwd, of door een wereldwijd vertrouwde CA, maar voor licenties wordt altijd een speciale Cisco Licensing Root CA gebruikt. Dit gebeurt automatisch zonder extra betrokkenheid van de gebruiker:



Deze CA wordt vertrouwd door Cisco-switches, maar niet door gewone client-pc's. Als u probeert om toegang te krijgen tot de URL voorgesteld door CSSM met behulp van een PC, toont de browser een fout als gevolg van het niet vertrouwen op de CA, maar de switch heeft geen problemen:



Als er echter een firewall is die SSL-inspectie uitvoert met certificaatspoofing tussen de switch en de CSM-server, vervangt de firewall het certificaat dat is ondertekend door Cisco CA, door een ander certificaat dat doorgaans is ondertekend door een Enterprise CA, die wordt vertrouwd door alle pc's en servers in de organisatie, maar niet door de switch. Zorg ervoor dat alle verkeer naar CSM wordt uitgesloten van HTTPS-inspectie.

Wanneer u problemen oplost met de "server TLS cert kan niet worden gevalideerd"-fout, hebt u toegang tot de URL die op de switch met een browser is geconfigureerd en controleert u of het certificaat correct is ondertekend door Cisco CA en de FQDN in de URL-string overeenkomt met de FQDN in het certificaat.

"Communicatiefout" of "Kan host niet oplossen: cslu-lokaal"

CSSM is doorgaans geconfigureerd met een FQDN in de URL en in de meeste Nexus implementaties is DNS niet geconfigureerd, wat vaak leidt tot dit type fout.

De eerste stap van het oplossen van problemen zou zijn om de geconfigureerde FQDN te pingen van de VRF die wordt gebruikt voor slimme licenties. Met deze configuratie bijvoorbeeld:

```
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
```

Deze fout geeft aan dat de DNS-resolutie in VRF-beheer niet werkt. Controleer de configuratie van de IP-naamserver onder de opgegeven VRF. Merk op dat DNS-serverconfiguratie per VRF is, zodat de ip name-server configuratie in de standaard VRF niet van kracht wordt in VRF-beheer. Als een stop-gap oplossing, ip-host kan worden gebruikt om een handmatige invoer toe te voegen, maar veronderstel dat in de toekomst het IP-adres van de server kan veranderen, en deze vermelding kan ongeldig worden.

Als de domeinnaam is opgelost, maar pings mislukt, kan dit worden veroorzaakt door een firewall die uitgaand pings blokkeert. In dit geval, kunt u Telnet gebruiken om te testen als poort 443 open is.

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

Als dit ook niet werkt, kunt u het netwerkpad naar de server problemen oplossen en ervoor zorgen dat het werkt.

"Fail to send out Call Home HTTP message"

Deze melding is fundamenteel vergelijkbaar met de melding "Communicatiefout". Het verschil is dat het over het algemeen wordt gezien op switches die erfenis Smart Licensing uitvoeren, niet

Smart Licensing met behulp van Beleid dat werd geïntroduceerd in NXOS release 10.2. Met erfenis Smart licentiëring, wordt de te benaderen URL geconfigureerd met behulp van de opdracht 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
```

Controleer of de configuratie correct is, HTTPS gebruikt en de URL (meestal tools.cisco.com) via de geselecteerde VRF bereikbaar is.

Verdere probleemoplossing

Raadpleeg Smart Licensing met Policy Troubleshooting voor datacenteroplossing voor een gedetailleerde controlelijst voor probleemoplossing met andere stappen die kunnen worden genomen om problemen met licenties op te lossen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.