Fehlerbehebung bei Lizenzierungsfehlern für Nexus 9000

Inhalt

Einleitung

In diesem Dokument werden die häufigsten Fehlertypen bei Smart Licensing für Switches der Serie Nexus 9000 beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Smart Licensing für Nexus Switches der Serie 9000
- Cisco Smart License Utility (CSLU)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Kommunikationsfehler

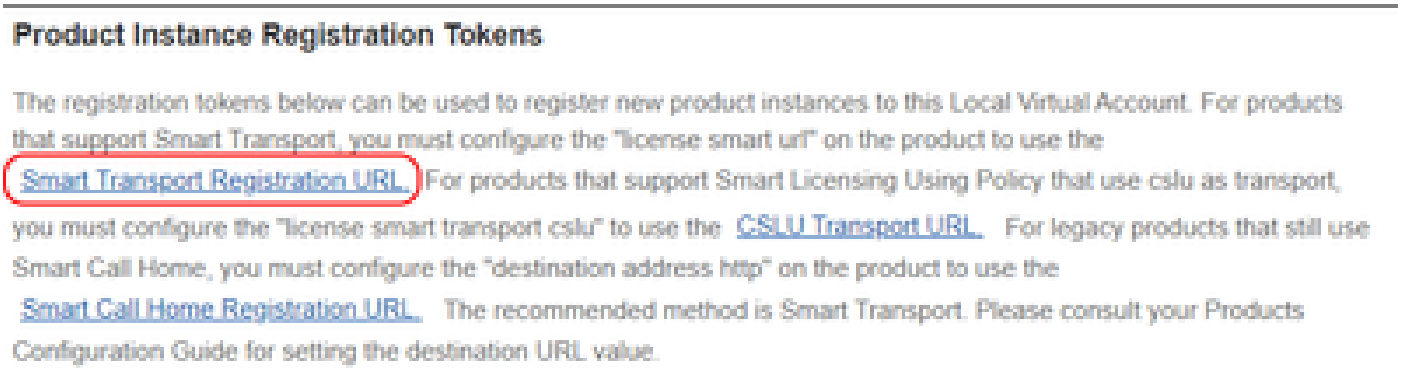
"Es kann keine sichere Verbindung hergestellt werden, da das TLS-Zertifikat des Servers nicht validiert werden kann."

Dieser CSLU-Fehler wird in der Regel entweder durch die Konfiguration eines falschen FQDN mit den Befehlen license smart url cslu oder license smart url smart oder durch ein Gerät im Pfad verursacht, das SSL-Spoofing ausführt (in der Regel eine Firewall mit aktivierter SSL-Überprüfung).

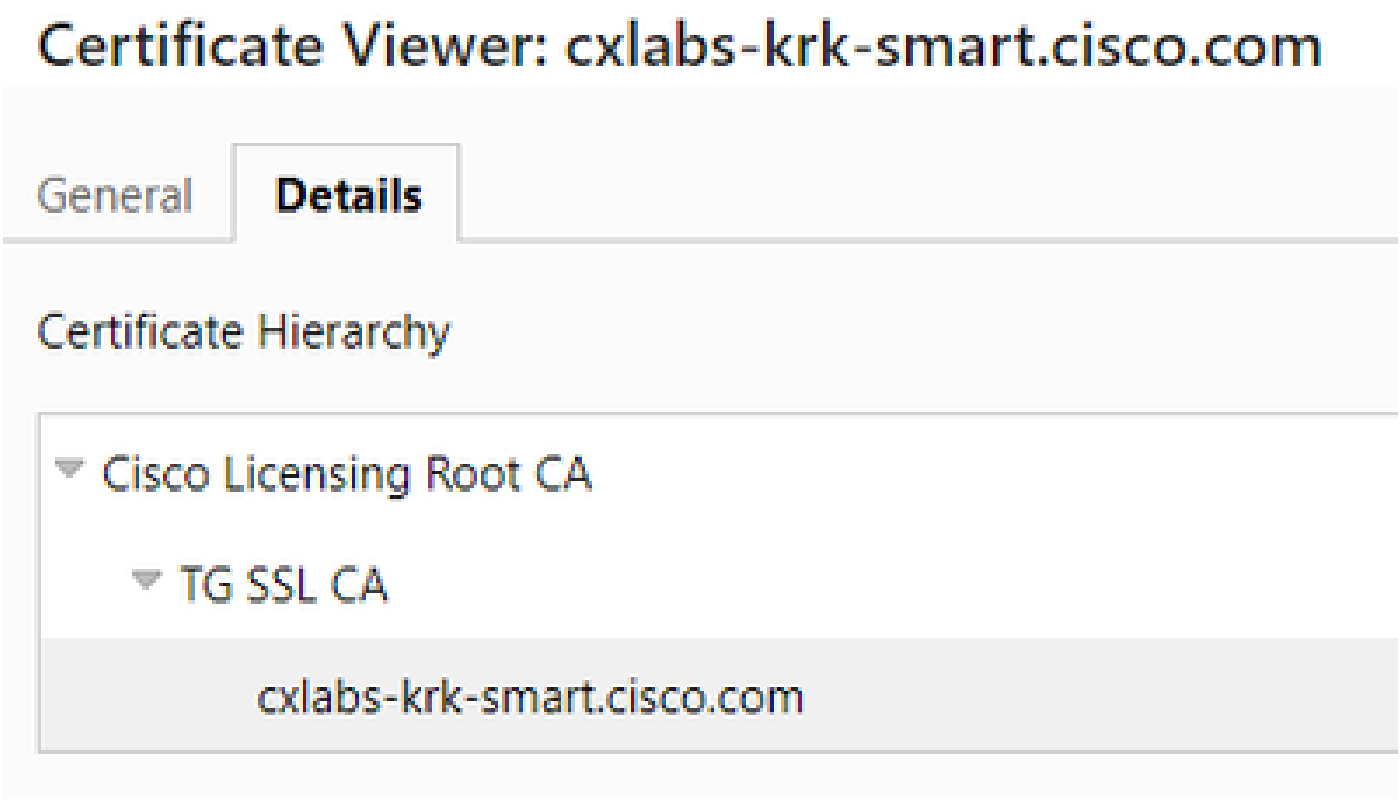
HTTPS unterscheidet sich auf einem Nexus-Switch nicht von anderen Systemen als auf einem typischen Client-Betriebssystem. Beim Zugriff auf eine HTTPS-Verbindung überprüft der Client den FQDN, auf den zugegriffen werden soll, anhand des FQDN, der im Zertifikat empfangen wurde - entweder das CN-Feld im Betreff-Header oder das SAN-Feld. Der Client überprüft außerdem, ob das empfangene Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde.

Wenn Sie versuchen, auf https://www.cisco.com zuzugreifen, öffnet Ihr Browser diese problemlos. Wenn Sie jedoch https://173.37.145.84 öffnen, erhalten Sie eine Warnung, dass die Verbindung nicht vertrauenswürdig ist, obwohl www.cisco.com zu 173.37.145.84 aufgelöst werden würde. Der Browser versucht, auf 173.37.145.84 zuzugreifen, aber "173.37.145 1.84" im vom Server vorgelegten Zertifikat, sodass das Zertifikat nicht als gültig gilt.

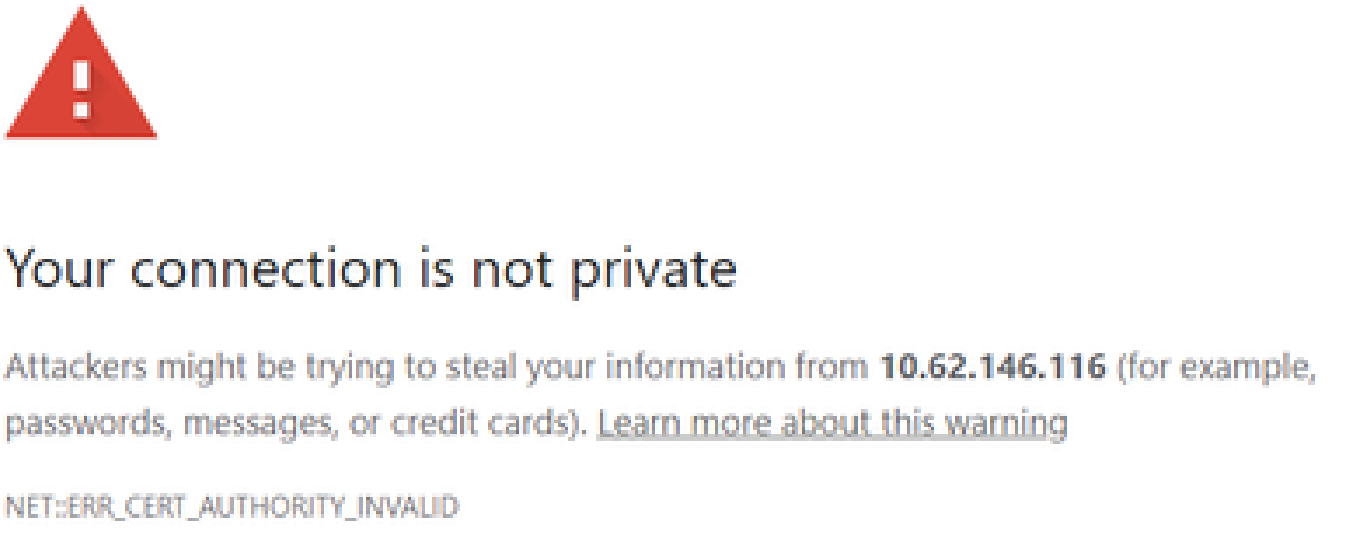
Aus diesem Grund muss bei der Konfiguration der CSSM-Adresse auf dem Switch unbedingt genau die vom CSSM selbst vorgeschlagene URL verwendet werden. Er enthält den in das Zertifikat eingebetteten FQDN:



Beachten Sie außerdem, dass für die standortbasierte CSSM-Verwaltung (standardmäßig Port 8443) und die Lizenzregistrierung (standardmäßig Port 443) separate Zertifikate verwendet werden. Das Verwaltungszertifikat kann selbstsigniert oder von einer lokalen, innerhalb der Organisation vertrauenswürdigen Unternehmenszertifizierungsstelle oder von einer global vertrauenswürdigen Zertifizierungsstelle signiert werden. Bei der Lizenzierung wird jedoch immer eine spezielle Cisco Lizenzierungs-Stammzertifizierungsstelle verwendet. Dies geschieht automatisch ohne zusätzlichen Benutzereingriff:



Diese CA wird von Cisco Switches als vertrauenswürdig angesehen, jedoch nicht von normalen Client-PCs. Wenn Sie versuchen, über einen PC auf die von CSSM vorgeschlagene URL zuzugreifen, zeigt der Browser einen Fehler an, da er der Zertifizierungsstelle nicht vertraut, aber der Switch hat keine Probleme:



Wenn es jedoch eine Firewall gibt, die SSL-Prüfungen mit Zertifikat-Spoofing zwischen dem Switch und dem CSSM-Server durchführt, ersetzt die Firewall das von der Cisco CA signierte Zertifikat durch ein anderes Zertifikat, das in der Regel von einer Unternehmenszertifizierungsstelle signiert wird, die von allen PCs und Servern in der Organisation als vertrauenswürdig angesehen wird, jedoch nicht vom Switch. Achten Sie darauf, jeglichen Datenverkehr an CSSM von der HTTPS-Prüfung auszuschließen.

Bei der Fehlerbehebung des Fehlers "Server-TLS-Zertifikat kann nicht validiert werden" greifen Sie mit einem Browser auf die auf dem Switch konfigurierte URL zu, und überprüfen Sie, ob das Zertifikat von der Cisco Zertifizierungsstelle ordnungsgemäß signiert wurde und der FQDN in der URL-Zeichenfolge mit dem FQDN im Zertifikat übereinstimmt.

"Kommunikationsfehler" oder "Der Host konnte nicht aufgelöst werden: cslu-local"

Der CSSM wird in der Regel mit einem FQDN in der URL konfiguriert, und in den meisten Nexus-Bereitstellungen ist DNS nicht konfiguriert, was häufig zu dieser Art von Fehler führt.

Der erste Schritt der Fehlerbehebung besteht darin, einen Ping an den konfigurierten FQDN der für Smart Licensing verwendeten VRF-Instanz zu senden. Beispiel für diese Konfiguration:

```
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
```

Dieser Fehler weist darauf hin, dass die DNS-Auflösung im VRF-Management nicht funktioniert. Überprüfen Sie die IP-Name-Server-Konfiguration unter der angegebenen VRF-Instanz. Die Konfiguration des DNS-Servers richtet sich nach VRF, daher wird die IP-Name-Server-Konfiguration im Standard-VRF in der VRF-Verwaltung nicht übernommen. Als Stopp-Gap-Lösung kann ip host verwendet werden, um einen manuellen Eintrag hinzuzufügen. Es wird jedoch davon ausgegangen, dass sich die IP-Adresse des Servers in Zukunft ändern kann, und dieser Eintrag kann ungültig werden.

Wenn der Domänenname aufgelöst wird, Pings jedoch fehlschlagen, könnte dies darauf zurückzuführen sein, dass eine Firewall ausgehende Pings blockiert. In diesem Fall können Sie Telnet verwenden, um zu testen, ob Port 443 offen ist.

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

Wenn auch dies nicht funktioniert, nehmen Sie eine Fehlerbehebung für den Netzwerkpfad zum Server vor, und stellen Sie sicher, dass dieser funktioniert.

"Fehler beim Senden der Call Home-HTTP-Nachricht"

Diese Meldung ähnelt im Wesentlichen der Meldung "Communications failure"

(Kommunikationsfehler). Der Unterschied besteht darin, dass dies im Allgemeinen auf Switches mit älterer Smart Licensing-Version zu beobachten ist, nicht bei Smart Licensing mit der in NXOS Version 10.2 eingeführten Richtlinie. Bei älterer Smart Licensing-Version wird die URL, auf die zugegriffen werden soll, mit dem callhome-Befehl konfiguriert.

```
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
```

Vergewissern Sie sich, dass die Konfiguration korrekt ist, HTTPS verwendet und die URL (in der Regel tools.cisco.com) über die ausgewählte VRF-Instanz erreichbar ist.

Weitere Fehlerbehebungsmaßnahmen

Eine detaillierte Checkliste zur Fehlerbehebung finden Sie unter Smart Licensing using Policy Troubleshooting on Data Center Solution. Sie enthält weitere Schritte zur Behebung von Lizenzproblemen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.