Dépannage des défaillances de licence sur Nexus 9000

Table des matières

Introduction

Ce document décrit les types d'erreurs les plus fréquemment rencontrés avec Smart Licensing sur les commutateurs de la gamme Nexus 9000.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Licences Smart sur les commutateurs de la gamme Nexus 9000
- Utilitaire de licence Cisco Smart (CSLU)

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Erreurs de défaillance des communications

"Impossible d'établir une connexion sécurisée car le certificat TLS du serveur ne

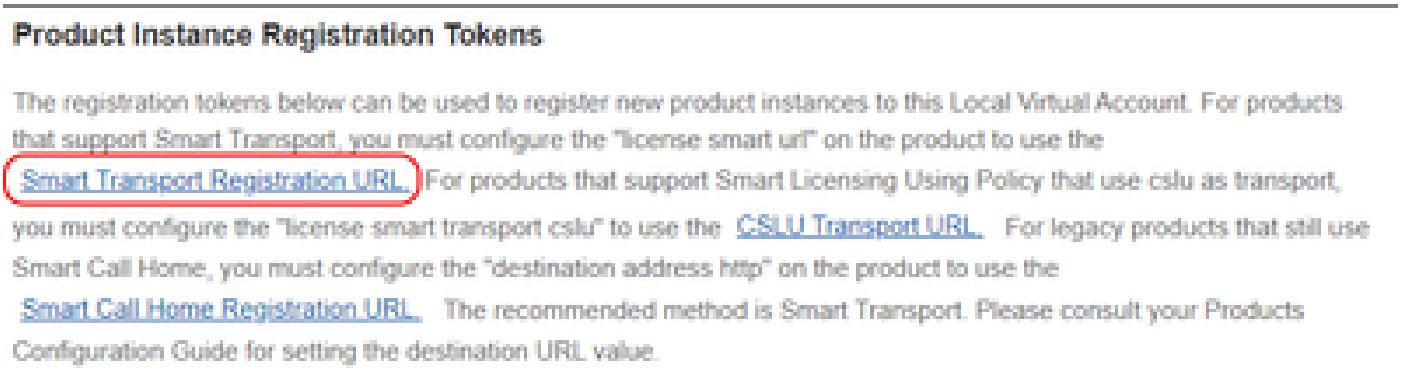
peut pas être validé"

Cette erreur CSLU est généralement provoquée soit par la configuration d'un FQDN incorrect en utilisant soit les commandes license smart url cslu ou license smart url smart, soit par un périphérique dans le chemin faisant une usurpation SSL (généralement un pare-feu avec l'inspection SSL activée).

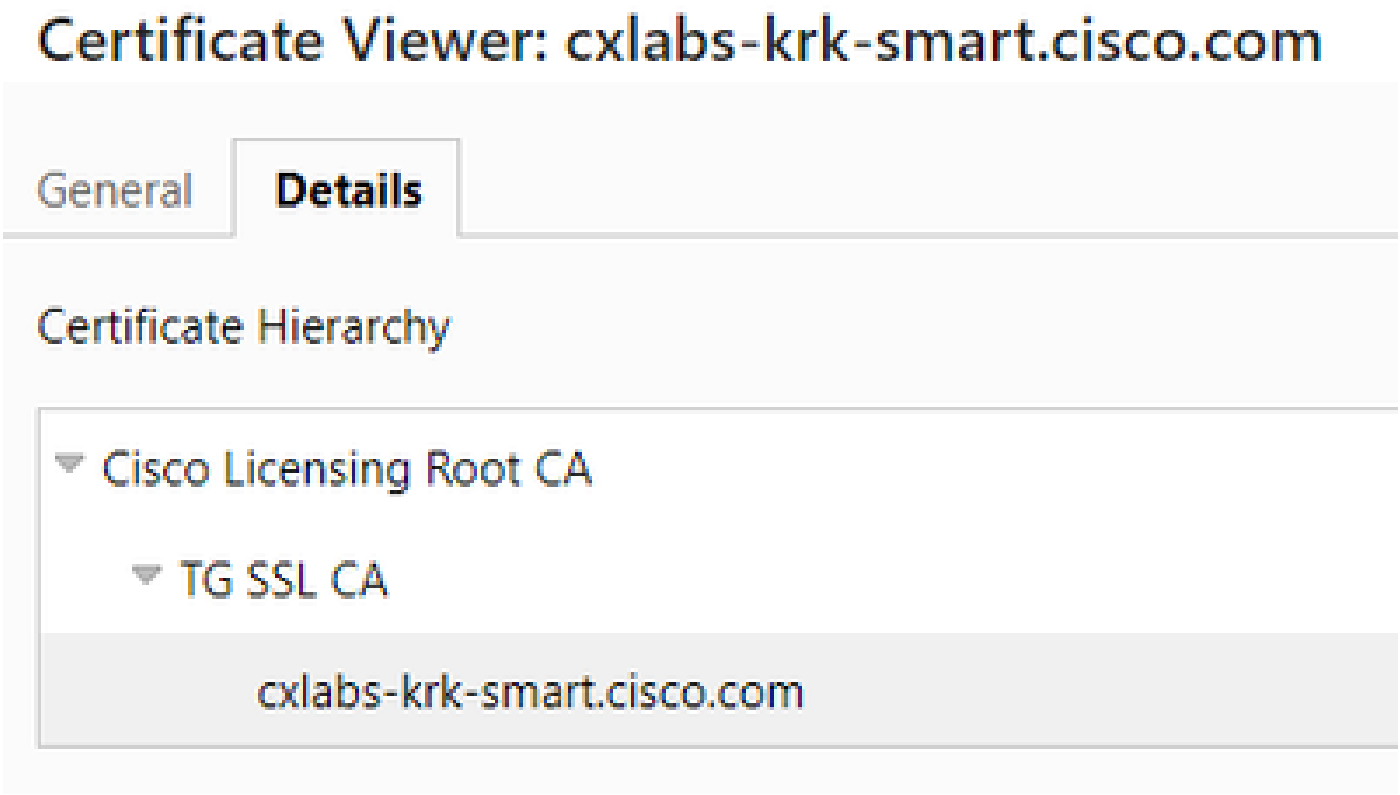
HTTPS sur un commutateur Nexus n'est pas différent de tout système d'exploitation client typique. Lors de l'accès à une liaison HTTPS, le client vérifie le nom de domaine complet auquel il tente d'accéder par rapport au nom de domaine complet reçu dans le certificat, soit le champ CN dans l'en-tête Subject, soit le champ SAN. Le client vérifie également si le certificat reçu est signé par une autorité de certification approuvée.

Si vous tentez d'accéder à https://www.cisco.com, votre navigateur l'ouvre sans problème. Cependant, si vous ouvrez https://173.37.145.84, vous obtenez un avertissement que la connexion ne peut pas être approuvée, même si www.cisco.com serait résolu à 173.37.145.84. Le navigateur tente d'accéder à 173.37.145.84, il ne voit pas « 173.37.145.84 » dans le certificat présenté par le serveur, de sorte que le certificat n'est pas considéré comme valide.

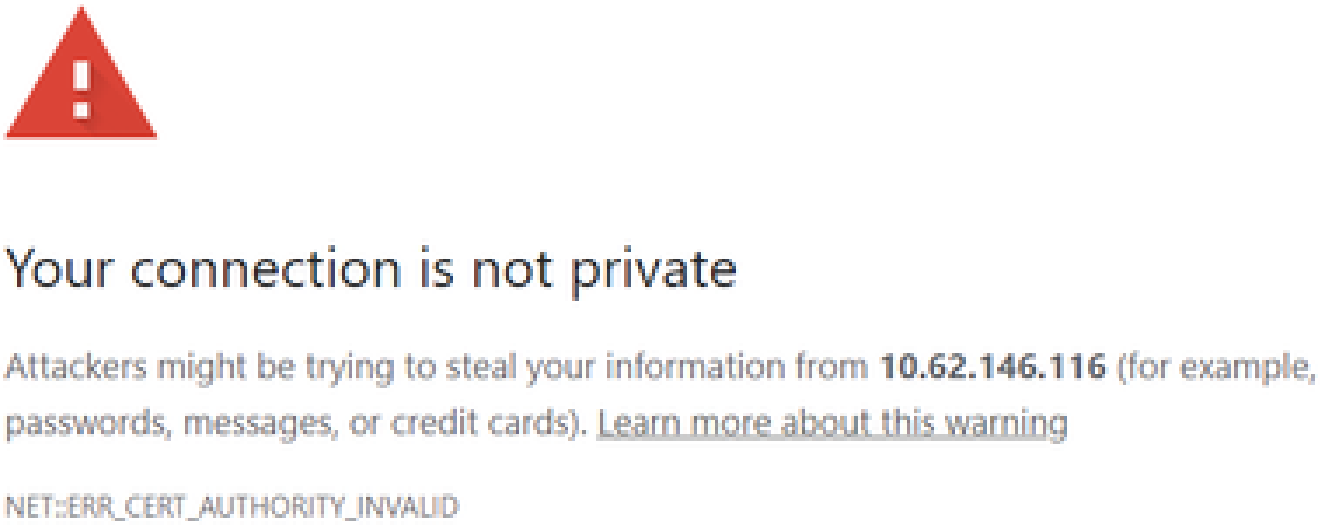
C'est pourquoi, lors de la configuration de l'adresse CSSM sur le commutateur, il est essentiel d'utiliser exactement l'URL proposée par CSSM lui-même ; il contient le nom de domaine complet intégré dans le certificat :



Il est également important de se rappeler qu'il existe des certificats distincts utilisés pour la gestion sur site de CSSM (port 8443 par défaut) et l'enregistrement de licence (port 443 par défaut). Le certificat de gestion peut être auto-signé, ou signé par une autorité de certification d'entreprise locale approuvée au sein de l'organisation, ou par une autorité de certification globalement approuvée, mais la licence utilise toujours une autorité de certification racine de licence Cisco spéciale. Cela se fait automatiquement sans intervention supplémentaire de l'utilisateur :



Cette autorité de certification est approuvée par les commutateurs Cisco, mais pas par les PC clients ordinaires. Si vous tentez d'accéder à l'URL proposée par CSSM à l'aide d'un PC, le navigateur affiche une erreur due à la non-approbation de l'autorité de certification, mais le commutateur n'a aucun problème :



Cependant, si un pare-feu effectue une inspection SSL avec usurpation de certificat entre le commutateur et le serveur CSSM, le pare-feu remplace le certificat signé par l'autorité de certification Cisco par un autre certificat signé généralement par une autorité de certification d'entreprise, qui est approuvée par tous les PC et serveurs de l'organisation, mais pas par le commutateur. Veillez à exclure tout trafic vers CSSM de l'inspection HTTPS.

Lors du dépannage de l'erreur « Le certificat TLS du serveur ne peut pas être validé », accédez à l'URL configurée sur le commutateur à l'aide d'un navigateur et vérifiez si le certificat est correctement signé par l'autorité de certification Cisco, et si le nom de domaine complet de la chaîne d'URL correspond au nom de domaine complet du certificat.

"Échec des communications" ou "Impossible de résoudre l'hôte : cslu-local"

Le CSSM est généralement configuré avec un nom de domaine complet dans l'URL, et dans la plupart des déploiements Nexus, DNS n'est pas configuré, ce qui entraîne souvent ce type de défaillance.

La première étape du dépannage consiste à envoyer une requête ping au nom de domaine complet configuré à partir du VRF utilisé pour Smart Licensing. Par exemple, avec cette configuration :

```
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
```

Cette erreur indique que la résolution DNS dans la gestion VRF ne fonctionne pas. Vérifiez la configuration ip name-server sous le VRF spécifié. Notez que la configuration du serveur DNS est par VRF, de sorte que la configuration ip name-server dans le VRF par défaut ne prend pas effet dans la gestion VRF. En tant que solution d'interruption, ip host peut être utilisé pour ajouter une entrée manuelle, mais supposez qu'à l'avenir, l'adresse IP du serveur peut changer et que cette entrée peut devenir non valide.

Si le nom de domaine est résolu, mais que les requêtes ping échouent, cela peut être dû au blocage des requêtes ping sortantes par un pare-feu. Dans ce cas, vous pouvez utiliser telnet pour vérifier si le port 443 est ouvert.

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

Si cela ne fonctionne pas non plus, dépannez le chemin réseau vers le serveur et assurez-vous qu'il fonctionne.

Échec de l'envoi du message HTTP Call Home

Ce message est fondamentalement similaire au message « Échec de la communication ». La différence est qu'il est généralement vu sur les commutateurs exécutant les licences Smart héritées, et non les licences Smart utilisant la stratégie qui a été introduite dans NXOS version 10.2. Avec les licences Smart héritées, l'URL à accéder est configurée en utilisant la commande 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
```

Assurez-vous que la configuration est correcte, qu'elle utilise HTTPS et que l'URL (généralement tools.cisco.com) est accessible sur le VRF sélectionné.

Dépannage supplémentaire

Reportez-vous à la section Licence intelligente utilisant le dépannage des stratégies sur la solution de centre de données pour obtenir une liste de contrôle de dépannage détaillée comprenant d'autres étapes qui pourraient être prises pour résoudre les problèmes liés à la licence.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.