

排除Nexus 9000上的許可故障

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[通訊故障錯誤](#)

["無法建立安全連線，因為無法驗證伺服器TLS證書"](#)

[「通訊故障」或「無法解析主機：cslu-local」](#)

["無法傳送Call Home HTTP消息"](#)

[其他疑難排解](#)

簡介

本文檔介紹Nexus 9000系列交換機上最常見的智慧許可錯誤型別。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Nexus 9000系列交換機上的智慧許可
- 思科智慧授權公用程式(CSLU)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

通訊故障錯誤

"無法建立安全連線，因為無法驗證伺服器TLS證書"

此CSLU錯誤通常是由以下原因造成的：使用license smart url cslu或license smart url smart命令配置不正確的FQDN，或者由路徑中的某些裝置執行SSL欺騙（通常是啟用SSL檢測的防火牆）導致。

Nexus交換機上的HTTPS與任何典型的客戶端作業系統上的相同。當訪問HTTPS連結時，客戶端將

驗證它嘗試訪問的FQDN是否與證書中接收的FQDN一致，即主題標頭中的CN欄位或SAN欄位。客戶端還驗證所接收的證書是否由受信任的證書頒發機構簽署。

如果您嘗試存取<https://www.cisco.com>，瀏覽器會順利開啟該頁面。但是，如果開啟<https://173.37.145.84>，會收到連線無法信任的警告，即使www.cisco.com會解析為173.37.145.84。瀏覽器正在嘗試訪問173.37.145.84，它不會在伺服器提供的證書中看到「173.37.145.84」，因此證書被視為無效。

因此，在交換器上設定CSSM位址時，必須準確使用CSSM本身提議的URL；它包含嵌入到證書中的FQDN：

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this Local Virtual Account. For products that support Smart Transport, you must configure the "license smart url" on the product to use the [Smart Transport Registration URL](#). For products that support Smart Licensing Using Policy that use csu as transport, you must configure the "license smart transport csu" to use the [CSU Transport URL](#). For legacy products that still use Smart Call Home, you must configure the "destination address http" on the product to use the [Smart Call Home Registration URL](#). The recommended method is Smart Transport. Please consult your Products Configuration Guide for setting the destination URL value.

此外，請務必記住，有單獨的證書用於CSSM內部管理（預設情況下為8443）和許可證註冊（預設情況下為443）。管理證書可以自簽名，或由組織內信任的本地企業CA或全域性信任的CA簽名，但授權始終使用特殊的思科授權根CA。此操作會自動完成，無需任何額外使用者參與：

Certificate Viewer: cxlabs-krk-smart.cisco.com

General

Details

Certificate Hierarchy

▼ Cisco Licensing Root CA

▼ TG SSL CA

cxlabs-krk-smart.cisco.com

此CA受Cisco交換機的信任，但普通客戶端PC不信任。如果您嘗試使用PC存取CSSM建議的URL，瀏覽器會顯示由於不信任CA而導致的錯誤，但交換器沒有任何問題：



Your connection is not private

Attackers might be trying to steal your information from **10.62.146.116** (for example, passwords, messages, or credit cards). [Learn more about this warning](#)

NET:ERR_CERT_AUTHORITY_INVALID

但是，如果存在在交換機和CSSM伺服器之間通過證書欺騙執行SSL檢查的防火牆，則防火牆會用通常由企業CA簽署的不同證書來替換由Cisco CA簽署的證書，企業CA是組織中的所有PC和伺服器所信任的，而不是由交換機所信任。請確保從HTTPS檢查中排除任何指向CSSM的流量。

疑難排解「伺服器TLS憑證無法驗證」錯誤時，請使用瀏覽器存取交換器上設定的URL，並檢查憑證是否由Cisco CA正確簽署，以及URL字串中的FQDN是否與憑證中的FQDN相符。

"通訊故障" 或 "無法解析主機：cslu-local"

CSSM通常在URL中配置有FQDN，而在大多數Nexus部署中，未配置DNS，這經常導致此類故障。

故障排除的第一步是從用於智慧許可的VRF對配置的FQDN執行ping。例如，使用以下設定：

```
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
```

此錯誤表示VRF管理中的DNS解析不起作用。在指定的VRF下驗證ip name-server配置。請注意，DNS伺服器配置是每個VRF，因此預設VRF中的ip name-server配置不會在VRF管理中生效。作為停止間隙解決方案，可以使用ip host新增手動條目，但假定在將來，伺服器的IP地址可能會更改，並且該條目可能變為無效。

如果域名解析了，但ping失敗，則可能是由於防火牆阻止傳出ping。在這種情況下，可以使用telnet測試埠443是否開啟。

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

如果這不起作用，請排查通向伺服器的網路路徑故障，確保它正常工作。

"無法傳送Call Home HTTP消息"

此消息與「通訊故障」消息基本相似。不同之處在於，它通常出現在運行舊版智慧許可的交換機上，而不是NXOS 10.2版中引入的使用策略的智慧許可。使用舊版智慧許可時，使用callhome 命令配置要訪問的URL。

```
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
```

確保配置正確，使用HTTPS，並且可以通過所選VRF訪問URL(通常為tools.cisco.com)。

其他疑難排解

請參閱[使用資料中心解決方案策略故障排除的智慧許可](#)，瞭解詳細的故障排除清單，該清單涉及解決與許可相關的問題可以採取的其他步驟。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。