排除Nexus 9000上的许可故障

目录

简介

本文档介绍Nexus 9000系列交换机上最常见的智能许可错误类型。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Nexus 9000系列交换机上的智能许可
- 思科智能许可证实用程序(CSLU)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

通信故障错误

"无法建立安全连接，因为无法验证服务器TLS证书"

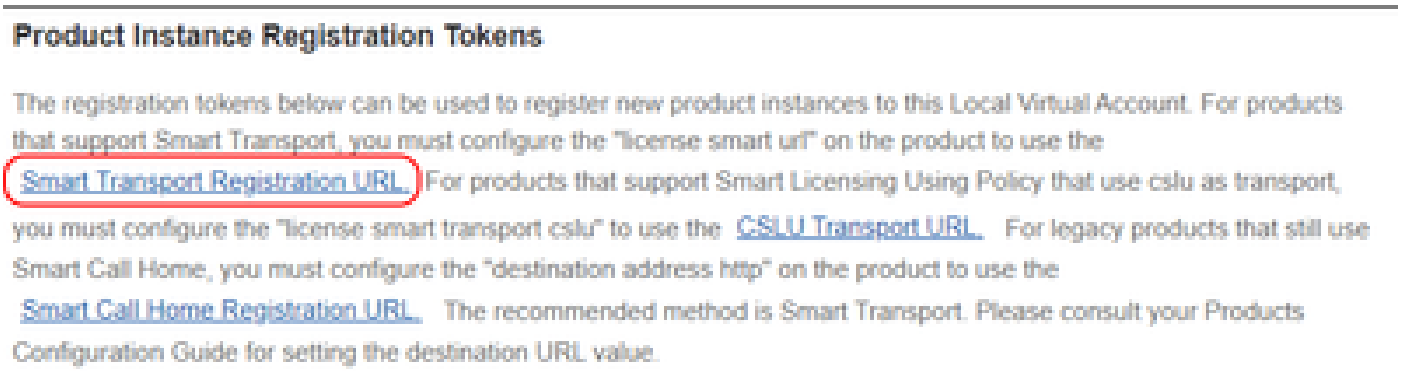
此CSLU错误通常是由以下原因造成的：使用license smart url cslu或license smart url smart命令配置错误的FQDN，或者由路径中的某些设备执行SSL欺骗（通常是启用SSL检查的防火墙）导致。

Nexus交换机上的HTTPS与任何典型的客户端操作系统上的HTTPS相同。当访问HTTPS链路时，客户端会根据证书中收到的FQDN（Subject标头中的CN字段或SAN字段）验证其尝试访问的

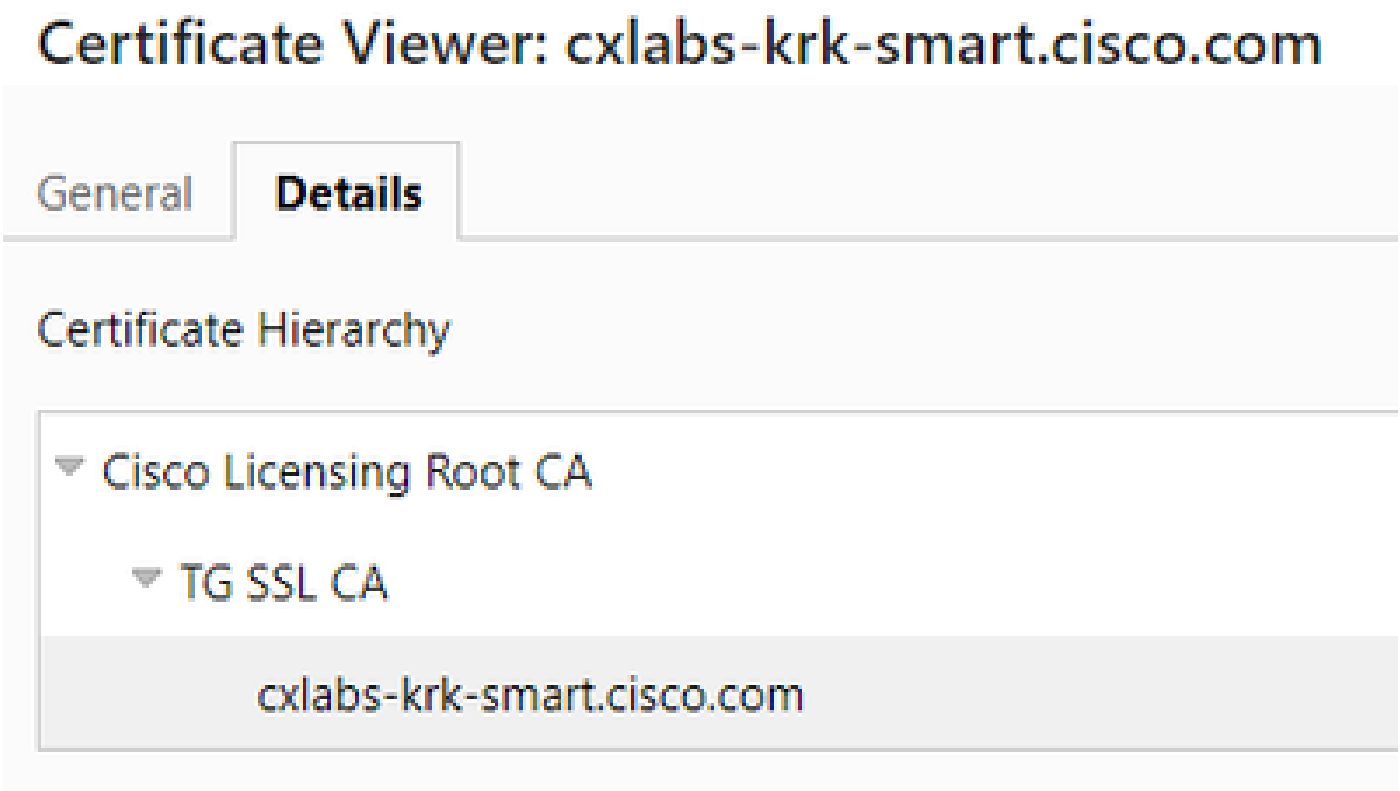
FQDN。客户端还验证收到的证书是否由受信任的证书颁发机构签名。

如果您尝试访问https://www.cisco.com,您的浏览器会打开它而不会出现问题。但是，如果打开https://173.37.145.84，您将收到连接不可信的警告，即使www.cisco.com会解析为173.37.145.84。浏览器正在尝试访问173.37.145.84，它不会在服务器提供的证书中看到“173.37.145.84”，因此证书被视为无效。

因此，在交换机上配置CSSM地址时，必须准确使用CSSM自身推荐的URL;它包含嵌入在证书中的FQDN:



此外，还必须记住，有单独的证书用于CSSM内部管理（默认情况下端口8443）和许可证注册（默认情况下端口443）。 管理证书可以自签名，或由组织内信任的本地企业CA或全局信任的CA签名，但许可始终使用特殊的思科许可根CA。此操作会自动完成，无需任何额外用户参与：



此CA受思科交换机的信任，但普通客户端PC不信任。如果您尝试使用PC访问CSSM提议的URL，浏览器会显示由于不信任CA而导致的错误，但交换机没有任何问题：

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，如果防火墙在交换机和CSSM服务器之间通过证书欺骗执行SSL检查，则防火墙会用通常由企业CA签署的另一证书替换由Cisco CA签署的证书，企业CA受组织内所有PC和服务器的信任，但交换机不信任。确保从HTTPS检查中排除任何指向CSSM的流量。

当排除“服务器TLS证书无法验证”错误时，请使用浏览器访问交换机上配置的URL，并检查证书是否由Cisco CA正确签名，并且URL字符串中的FQDN与证书中的FQDN匹配。

"通信故障”或“无法解析主机：cslu-local”

CSSM通常使用URL中的FQDN进行配置，而在大多数Nexus部署中，未配置DNS，这经常会导致此类故障。

故障排除的第一步是从用于智能许可的VRF ping配置的FQDN。例如，使用此配置：

```
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
```

此错误表示VRF管理中的DNS解析不起作用。验证指定VRF下的ip name-server配置。请注意，DNS服务器配置是按VRF进行的，因此默认VRF中的ip name-server配置不会在VRF管理中生效。作为停止间隙解决方案，可以使用ip host添加手动条目，但假设在将来，服务器的IP地址可能会更改，并且该条目可能变为无效。

如果域名解析了，但ping失败，则这可能是由于防火墙阻止传出ping造成的。在这种情况下，您可以使用telnet测试端口443是否打开。

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

如果这也行不通，请对通向服务器的网络路径进行故障排除并确保它行得通。

"无法发送Call Home HTTP消息"

此消息从根本上类似于“通信故障”消息。区别在于，通常在运行旧版智能许可的交换机上看到它，而不是使用NXOS版本10.2中引入的策略进行智能许可。使用旧版智能许可时，使用callhome命令配置要访问的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
```

确保配置正确且使用HTTPS，并且可通过所选VRF访问URL(通常为tools.cisco.com)。

进一步排除故障

请参阅使用数据中心解决方案策略故障排除的智能许可，了解详细的故障排除核对表，该核对表涉及解决许可相关问题可以采取的其他步骤。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。