Nexus 9000의 라이센싱 오류 트러블슈팅

목차

소개

이 문서에서는 Nexus 9000 시리즈 스위치의 Smart Licensing에서 가장 일반적으로 나타나는 오류 유형에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

통신 실패 오류

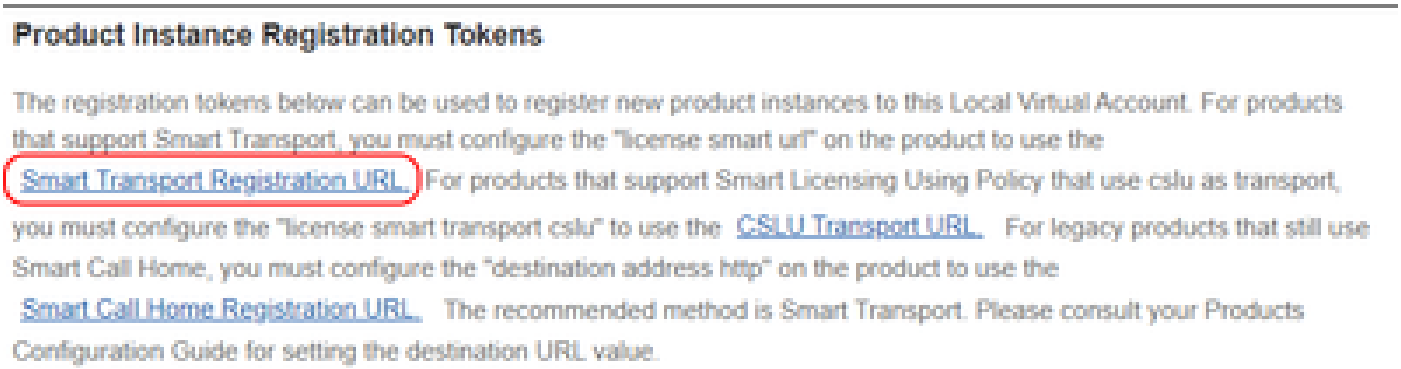
"서버 TLS 인증서를 확인할 수 없으므로 보안 연결을 설정할 수 없습니다."

이 CSLU 오류는 일반적으로 라이센스 smart url cslu 또는 라이센스 smart url smart 명령 중 하나를 사용하여 잘못된 FQDN을 구성하거나 SSL 스푸핑을 수행하는 경로의 일부 디바이스(일반적으로 SSL 검사가 활성화된 방화벽)에서 발생합니다.

Nexus 스위치의 HTTPS는 일반적인 클라이언트 OS와 다르지 않습니다. HTTPS 링크에 액세스할 때 클라이언트는 인증서에 수신된 FQDN(주체 헤더의 CN 필드 또는 SAN 필드)에 대해 액세스하려는 FQDN을 확인합니다. 클라이언트는 또한 수신된 인증서가 신뢰할 수 있는 인증 기관에서 서명되었는지 확인합니다.

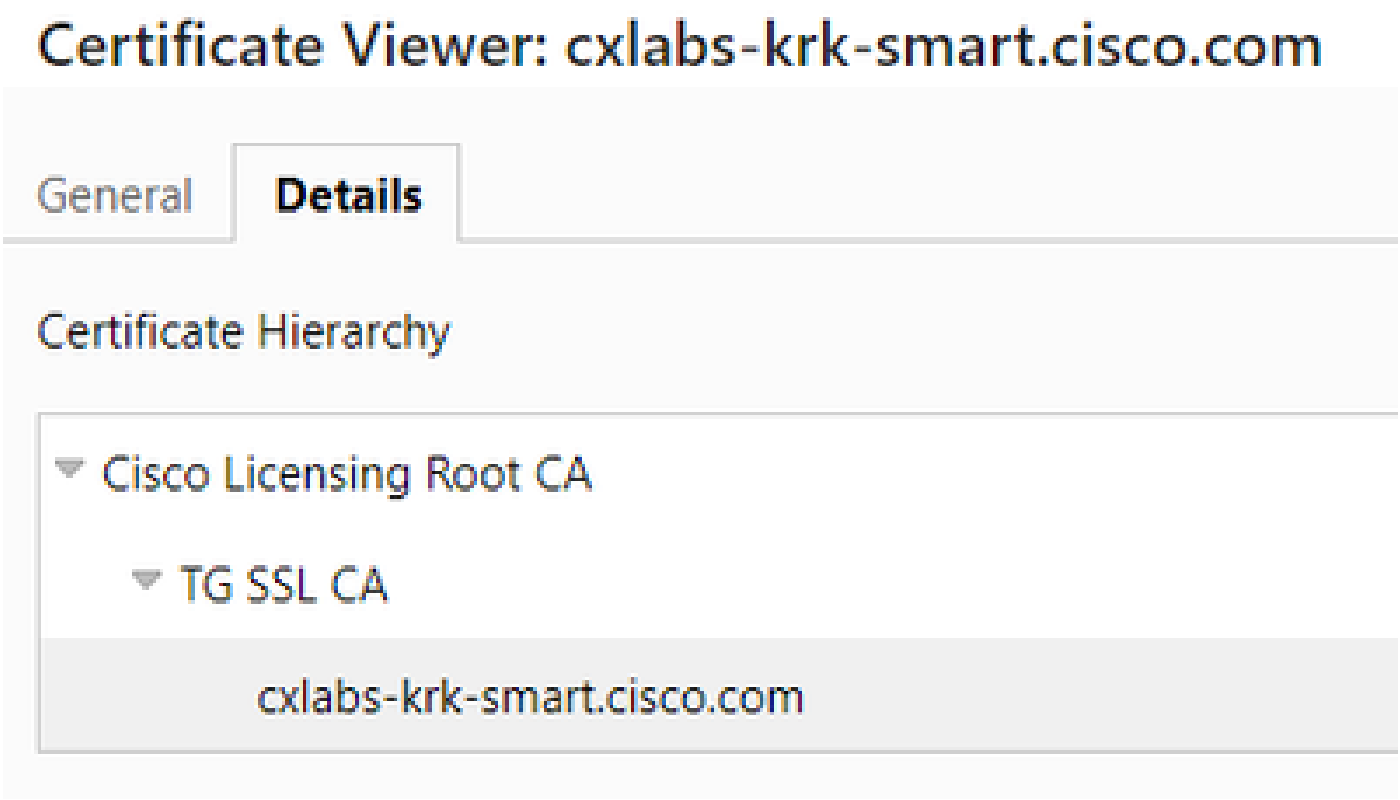
https://www.cisco.com에 액세스하려고 하면 브라우저에서 아무 문제 없이 열립니다. 그러나 https://173.37.145.84을 열면 www.cisco.com이 173.37.145.84로 확인되더라도 연결을 신뢰할 수 없다는 경고 메시지가 표시됩니다. 브라우저가 173.37.145.84에 액세스하려고 하지만 서버에서 제공하는 인증서에 "173.37.145.84"가 표시되지 않으므로 인증서가 유효한 것으로 간주되지 않습니다.

따라서 스위치에서 CSSM 주소를 구성할 때 CSSM 자체에서 제안하는 URL을 정확하게 사용해야 합니다. 인증서에 포함된 FQDN을 포함합니다.

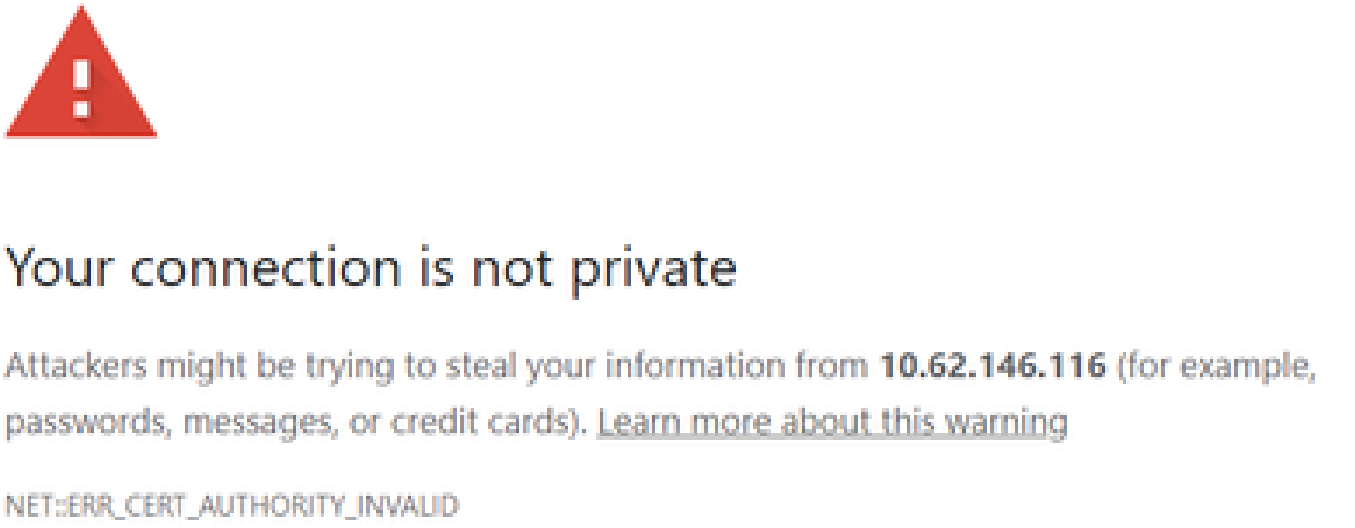

Product Instance Registration Tokens

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 cslu as transport, you must configure the "license smart transport cslu" to use the CSLU 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.

CSSM 온프레미스 관리(기본적으로 포트 8443) 및 라이센스 등록(기본적으로 포트 443)에 사용되는 별도의 인증서가 있다는 점도 기억해야 합니다. 관리 인증서는 자체 서명 또는 조직 내에서 신뢰할 수 있는 로컬 엔터프라이즈 CA나 세계적으로 신뢰할 수 있는 CA가 서명할 수 있지만, 라이센싱은 항상 특별한 Cisco Licensing Root CA를 사용합니다. 이 작업은 추가 사용자 개입 없이 자동으로 수행됩니다.



이 CA는 Cisco 스위치에서 신뢰하지만 일반 클라이언트 PC에서는 신뢰하지 않습니다. CSSM이 PC를 사용하여 제안한 URL에 액세스하려고 하면 CA를 신뢰하지 않아 브라우저에 오류가 표시되지만 스위치에는 문제가 없습니다.



그러나 스위치와 CSSM 서버 간에 인증서 스푸핑이 포함된 SSL 검사를 수행하는 방화벽이 있는 경우, 방화벽은 Cisco CA가 서명한 인증서를 엔터프라이즈 CA가 서명한 다른 인증서로 교체합니다. 엔터프라이즈 CA는 조직의 모든 PC 및 서버에서 신뢰하지만 스위치에서는 신뢰하지 않습니다. HTTPS 검사에서 CSSM에 대한 트래픽을 제외해야 합니다.

"서버 TLS 인증서의 유효성을 검사할 수 없음" 오류를 해결할 때 브라우저에서 스위치에 구성된 URL에 액세스하여 인증서가 Cisco CA에 의해 올바르게 서명되었는지, URL 문자열의 FQDN이 인

증서의 FQDN과 일치하는지 검사합니다.

"통신 실패" 또는 "호스트를 확인할 수 없음: cslu-local"

CSSM은 일반적으로 URL의 FQDN으로 구성되며, 대부분의 Nexus 구축에서는 DNS가 구성되지 않으므로 이러한 유형의 장애가 자주 발생합니다.

트러블슈팅의 첫 번째 단계는 Smart Licensing에 사용되는 VRF에서 구성된 FQDN을 ping하는 것입니다. 예를 들어, 이 컨피그레이션에서는

```
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
```

이 오류는 VRF 관리에서 DNS 확인이 작동하지 않음을 나타냅니다. 지정된 VRF에서 ip 이름-서버 컨피그레이션을 확인합니다. DNS 서버 컨피그레이션은 VRF별로 이루어지므로 기본 VRF의 ip 이름-서버 컨피그레이션은 VRF 관리에서 적용되지 않습니다. Stop-Gap 솔루션으로서 ip 호스트를 사용하여 수동 항목을 추가할 수 있지만 나중에 서버의 IP 주소가 변경될 수 있으며 이 항목은 무효화될 수 있다고 가정합니다.

도메인 이름이 확인되었지만 ping이 실패한 경우, 이는 방화벽이 발신 ping을 차단하기 때문에 발생할 수 있습니다. 이 경우 텔넷을 사용하여 포트 443이 열려 있는지 테스트할 수 있습니다.

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

둘 중 하나라도 작동하지 않을 경우 서버에 대한 네트워크 경로를 트러블슈팅하고 제대로 작동하는지 확인합니다.

"Call Home HTTP 메시지를 보내지 못했습니다"

이 메시지는 기본적으로 "통신 실패" 메시지와 유사합니다. 차이점은 일반적으로 NXOS 릴리스 10.2에 도입된 정책을 사용하는 스마트 라이센싱이 아니라 레거시 스마트 라이센싱을 실행하는 스위치에서 나타난다는 점입니다. 레거시 스마트 라이센싱에서는 callhome 명령을 사용하여 액세스할 URL이 구성됩니다.

```
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
```

컨피그레이션이 올바르고 HTTPS를 사용하며, 선택한 VRF를 통해 URL(일반적으로 tools.cisco.com)에 연결할 수 있는지 확인합니다.

추가 문제 해결

라이센싱과 관련된 문제를 해결하기 위해 수행할 수 있는 다른 단계와 관련된 자세한 문제 해결 체크리스트에 대해서는 Smart Licensing using Policy Troubleshooting on Data Center Solution을 참조하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.