Solucione problemas de falhas de licenciamento do Nexus 9000

Contents

Introdução

Este documento descreve os tipos de erros mais comumente vistos com o Smart Licensing nos switches Nexus 9000 Series.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Smart Licensing no switch Nexus 9000 series
- Cisco Smart License Utility (CSLU)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Erros de falha de comunicação

"Não é possível estabelecer conexão segura porque o certificado TLS do servidor

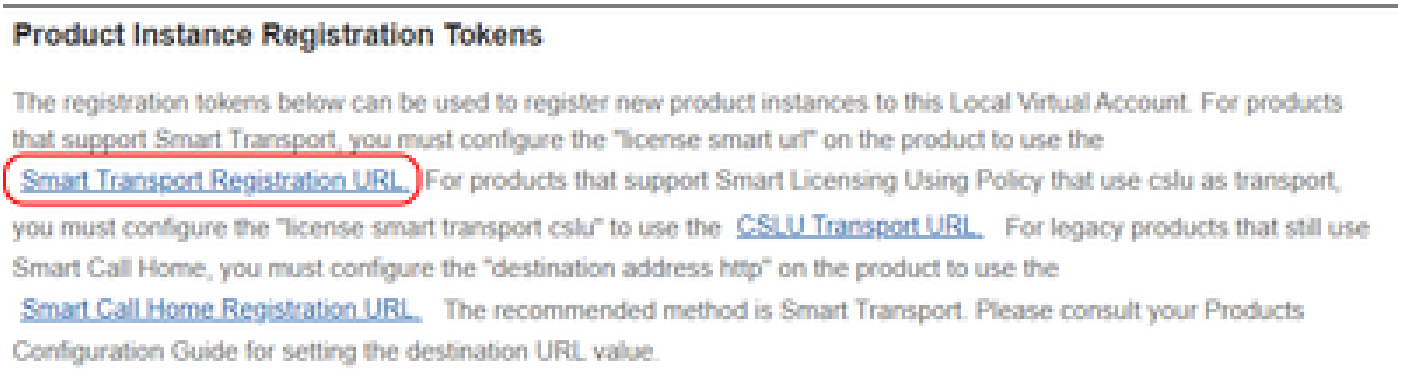
não pode ser validado"

Esse erro de CSLU é normalmente causado pela configuração de um FQDN incorreto usando os comandos license smart url cslu ou license smart url smart, ou por algum dispositivo no caminho que faz spoofing de SSL (normalmente um firewall com inspeção de SSL habilitada).

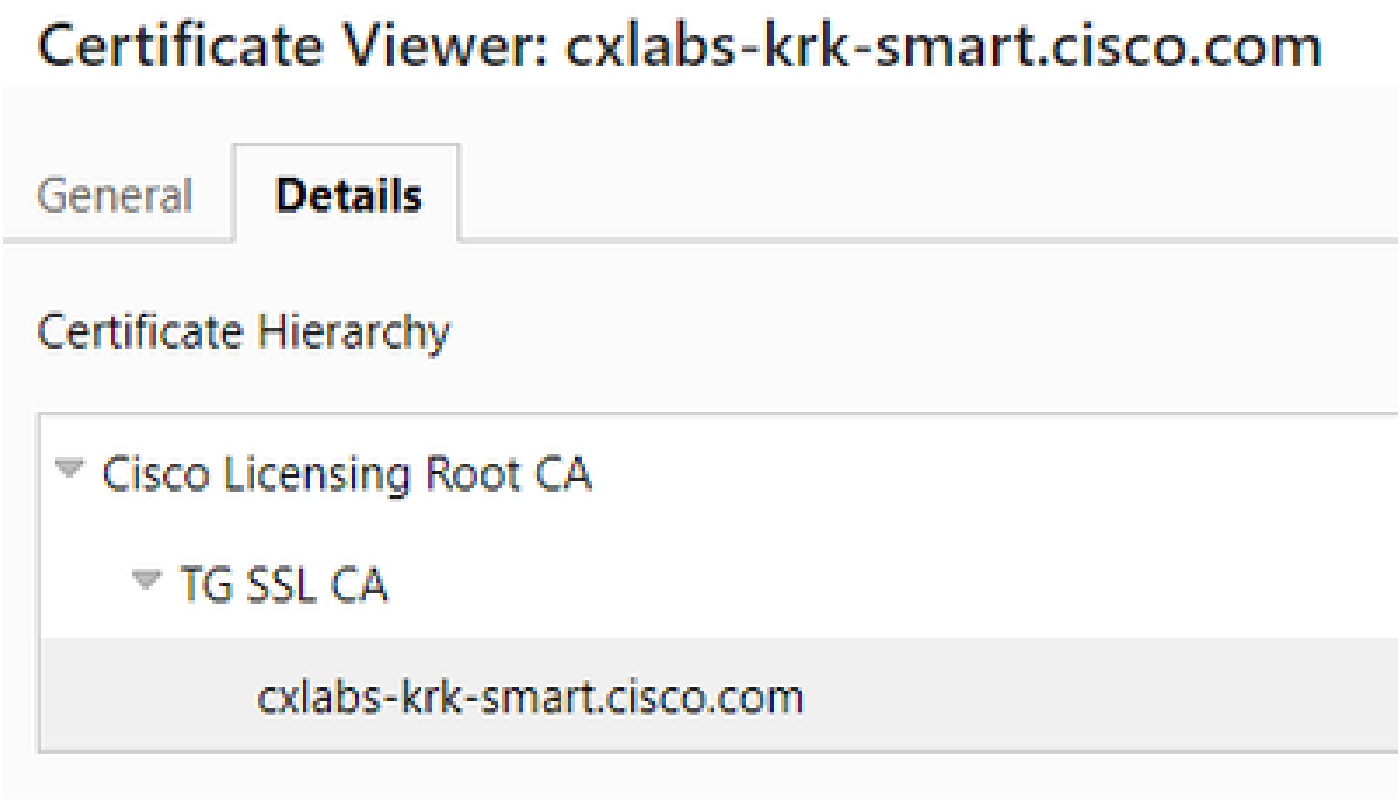
O HTTPS em um switch Nexus não é diferente do que em qualquer SO cliente típico. Ao acessar um link HTTPS, o cliente verificaria o FQDN que está tentando acessar em relação ao FQDN recebido no certificado - o campo CN no cabeçalho Assunto ou o campo SAN. O cliente também valida se o certificado recebido está assinado por uma autoridade de certificação confiável.

Se você tentar acessar https://www.cisco.com, seu navegador o abrirá sem problemas. No entanto, se você abrir https://173.37.145.84, receberá um aviso de que a conexão não é confiável, mesmo que www.cisco.com seja resolvido para 173.37.145.84. O navegador está tentando acessar 173.37.145.84, ele não vê "173.37.145.84" no certificado apresentado pelo servidor, portanto, o certificado não é considerado válido.

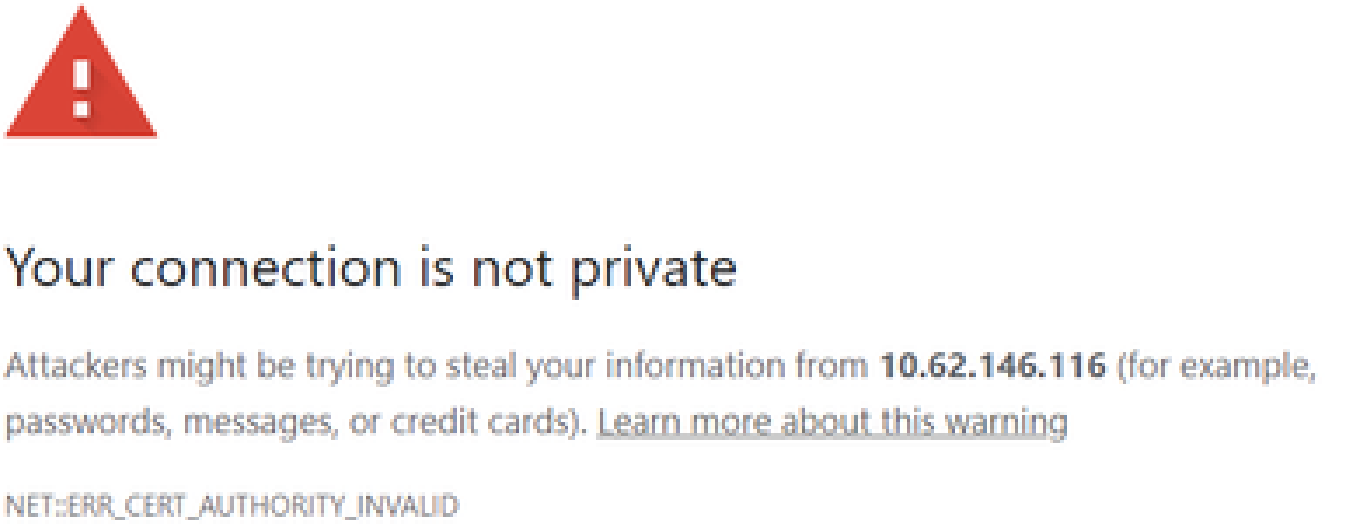
É por isso que, ao configurar o endereço CSSM no switch, é essencial usar exatamente o URL proposto pelo próprio CSSM; ele contém o FQDN incorporado no certificado:



Também é importante lembrar que há certificados separados usados para o gerenciamento local do CSSM (porta 8443 por padrão) e o registro de licença (porta 443 por padrão). O certificado de gerenciamento pode ser autoassinado ou assinado por uma CA corporativa local confiável na organização ou por uma CA globalmente confiável, mas o licenciamento sempre usa uma CA raiz de licenciamento da Cisco especial. Isso é feito automaticamente, sem qualquer envolvimento adicional do usuário:



Essa CA é confiável para os switches Cisco, mas não para os PCs cliente comuns. Se você tentar acessar o URL proposto pelo CSSM usando um PC, o navegador exibirá um erro por não confiar no CA, mas o switch não terá nenhum problema:



No entanto, se houver um firewall fazendo inspeção SSL com falsificação de certificado entre o switch e o servidor CSSM, o firewall substituirá o certificado assinado pela CA da Cisco por um certificado diferente assinado geralmente por uma CA corporativa, que é confiável para todos os PCs e servidores na organização, mas não pelo switch. Certifique-se de excluir qualquer tráfego para CSSM da inspeção HTTPS.

Ao solucionar o erro "certificado TLS do servidor não pode ser validado", acesse o URL

configurado no switch com um navegador e verifique se o certificado foi assinado corretamente pela CA da Cisco, e se o FQDN na string do URL corresponde ao FQDN no certificado.

"Falha de comunicação" ou "Não foi possível resolver o host: cslu-local"

O CSSM normalmente é configurado com um FQDN no URL e, na maioria das implantações do Nexus, o DNS não é configurado, o que frequentemente leva a esse tipo de falha.

A primeira etapa da solução de problemas seria executar um ping do FQDN configurado a partir do VRF usado para Smart Licensing. Por exemplo, com esta configuração:

```
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
```

Esse erro indica que a resolução DNS no gerenciamento de VRF não funciona. Verifique a configuração do ip name-server no VRF especificado. Observe que a configuração do servidor DNS é por VRF, portanto a configuração do ip name-server no VRF padrão não tem efeito no VRF Management. Como uma solução de intervalo de parada, o host IP pode ser usado para adicionar uma entrada manual, mas suponha que no futuro, o endereço IP do servidor possa mudar, e essa entrada pode se tornar inválida.

Se o nome de domínio for resolvido, mas os pings falharem, isso pode ser causado por um firewall que bloqueia pings de saída. Nesse caso, você pode usar o telnet para testar se a porta 443 está aberta.

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

Se isso também não funcionar, solucione os problemas do caminho de rede em direção ao servidor e verifique se ele funciona.

"Falha ao enviar mensagem HTTP do Call Home"

Essa mensagem é fundamentalmente semelhante à mensagem "Communications failure". A diferença é que geralmente ela é vista em switches que executam Smart Licensing legado, não Smart Licensing usando Política que foi introduzida no NXOS versão 10.2. Com o Smart Licensing legado, o URL a ser acessado é configurado usando o comando 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
```

Verifique se a configuração está correta, se usa HTTPS e se há acessibilidade ao URL (normalmente tools.cisco.com) no VRF selecionado.

Mais soluções de problemas

Consulte Smart Licensing using Policy Troubleshooting on Data Center Solution para obter uma lista de verificação detalhada de solução de problemas envolvendo outras etapas que podem ser executadas para resolver problemas relacionados ao licenciamento.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.