Nexus 9000のライセンス障害のトラブルシューティング

内容

はじめに

このドキュメントでは、Nexus 9000シリーズスイッチのスマートライセンスで最もよく見られるエラーのタイプについて説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Nexus 9000シリーズスイッチのスマートライセンス
- Ciscoスマートライセンスユーティリティ(CSLU)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

通信障害エラー

「サーバのTLS証明書を検証できないため、セキュアな接続を確立できません」

このCSLUエラーは通常、license smart url csluまたはlicense smart url smartコマンドを使用して誤ったFQDNを設定するか、パス内のデバイスがSSLスプーフィング（通常はSSLインスペクションが有効なファイアウォール）を実行したことが原因で発生します。

NexusスイッチのHTTPSは、一般的なクライアントOSのHTTPSと同じです。HTTPSリンクにアクセスするとき、クライアントはアクセスしようとしているFQDNを、証明書で受信したFQDN（SubjectヘッダーのCNフィールドまたはSANフィールド）と照合します。クライアントは、受信した証明書が信頼できる証明機関によって署名されているかどうかも検証します。

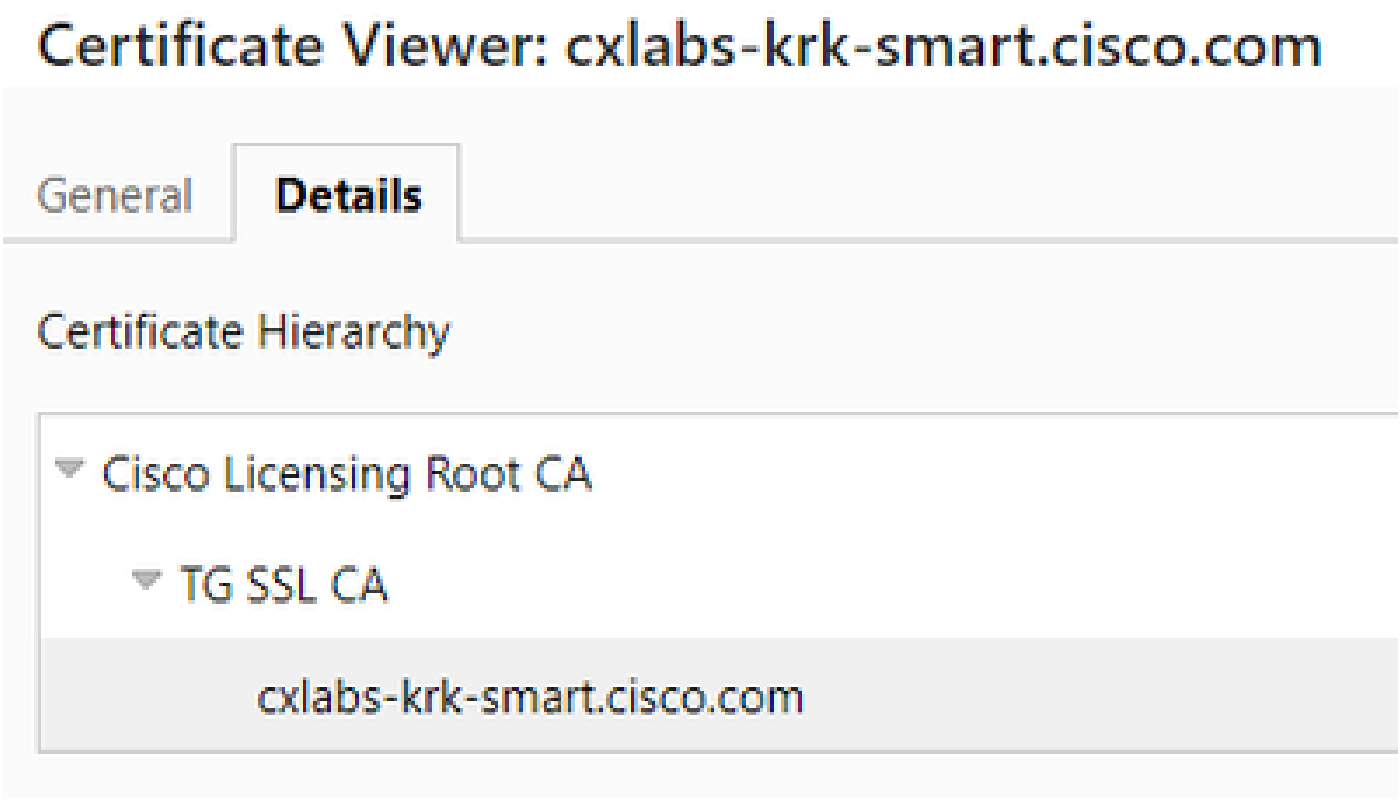
https://www.cisco.comにアクセスしようとすると、ブラウザが問題なく開きます。ただし、https://173.37.145.84を開くと、www.cisco.comが173.37.145.84に解決されるにもかかわらず、接続を信頼できないという警告が表示されます。ブラウザは173.37.145.84にアクセスしようとしますが、サーバから提示された証明書に「173.37.145.84」が表示されないため、証明書は有効であると見なされません。

このため、スイッチでCSSMアドレスを設定する際には、CSSM自体によって提示されたURLを正確に使用することが重要です。このURLには、証明書に埋め込まれたFQDNが含まれています。

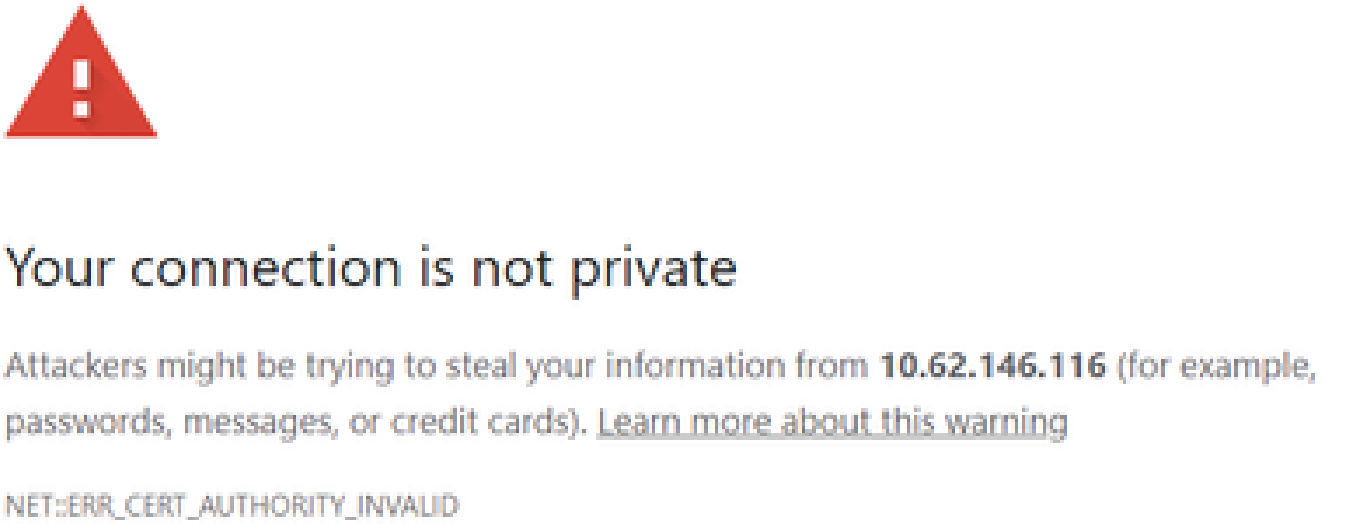
Product Instance Registration Tokens

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.

また、CSSMオンプレミス管理（デフォルトではポート8443）とライセンス登録（デフォルトではポート443）に対して個別の証明書が使用されることにも注意する必要があります。 管理証明書は自己署名するか、組織内で信頼されているローカルエンタープライズCAまたはグローバルに信頼されているCAによって署名することができますが、ライセンスは常に特別なシスコライセンシングルートCAを使用します。この処理は、ユーザの介入なしに自動的に実行されます。



このCAは、シスコのスイッチでは信頼されますが、通常のクライアントPCでは信頼されません。PCを使用してCSSMによって提示されたURLにアクセスしようとすると、CAを信頼していないためにブラウザにエラーが表示されますが、スイッチには問題がありません。



ただし、スイッチとCSSMサーバの間で証明書スプーフィングを使用してSSLインスペクションを実行しているファイアウォールがある場合、ファイアウォールは、Cisco CAによって署名された証明書を、通常はエンタープライズCAによって署名された別の証明書に置き換えます。エンタープライズCAは、スイッチではなく、組織内のすべてのPCとサーバによって信頼されています。HTTPSインスペクションからCSSMへのトラフィックを必ず除外してください。

「server TLS cert cannot be validated」エラーのトラブルシューティングを行う際には、スイッ

チに設定されたURLにブラウザでアクセスし、証明書がCisco CAによって正しく署名され、URL文字列のFQDNが証明書内のFQDNと一致するかどうかを検査します。

"Communications failure」または「ホストcslu-localを解決できませんでした。

CSSMは通常、URL内のFQDNで設定され、ほとんどのNexus展開ではDNSが設定されていないため、このタイプの障害が頻繁に発生します。

トラブルシューティングの最初のステップは、スマートライセンスに使用されるVRFから、設定されたFQDNにpingを実行することです。たとえば、次の設定を使用します。

```
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
```

このエラーは、VRF管理でのDNS解決が機能していないことを示しています。指定したVRFの下でのip name-server設定を確認します。DNSサーバの設定はVRF単位で行われるため、デフォルトVRFでのip name-server の設定はVRF管理では有効になりません。応急処置として、ip host を使用して手動エントリを追加できますが、将来、サーバのIPアドレスが変更されて、このエントリが無効になる可能性があると仮定します。

ドメイン名が解決されてもpingが失敗する場合は、ファイアウォールが発信pingをブロックしていることが原因である可能性があります。この場合、Telnetを使用して、ポート443が開いているかどうかをテストできます。

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

それでも問題が解決しない場合は、サーバへのネットワークパスをトラブルシューティングし、それが機能することを確認します。

"Fail to send out Call Home HTTP message"

このメッセージは、基本的に「通信障害」メッセージと似ています。異なる点は、一般的にNXOSリリース10.2で導入されたポリシーを使用するスマートライセンスではなく、従来のスマートライセンスを実行するスイッチで見られることです。従来のスマートライセンスでは、アクセスされるURLはcallhomeコマンドを使用して設定されます。

```
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
```

設定が正しいこと、HTTPSを使用していること、および選択したVRFを介してURL(通常はtools.cisco.com)に到達できることを確認します。

さらなるトラブルシューティング

ライセンスに関連する問題を解決するために実行できるその他の手順を含む詳細なトラブルシューティングチェックリストについては、「データセンターソリューションでのポリシーのトラブルシューティングを使用したスマートライセンス」を参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。