17.3.2以降にアップグレードした後のCatalyst 9000でのポリシーによるスマートライセンス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、最新のCisco IOS® XE 17.3.2にアップグレードした後の、Cat9kファミリのCatalystプラットフォームに関連する問題について説明します。

前提条件

要件

Cisco IOS XEデバイスでのSmart Licensingの操作に関する知識があることが推奨されます。

使用するコンポーネント

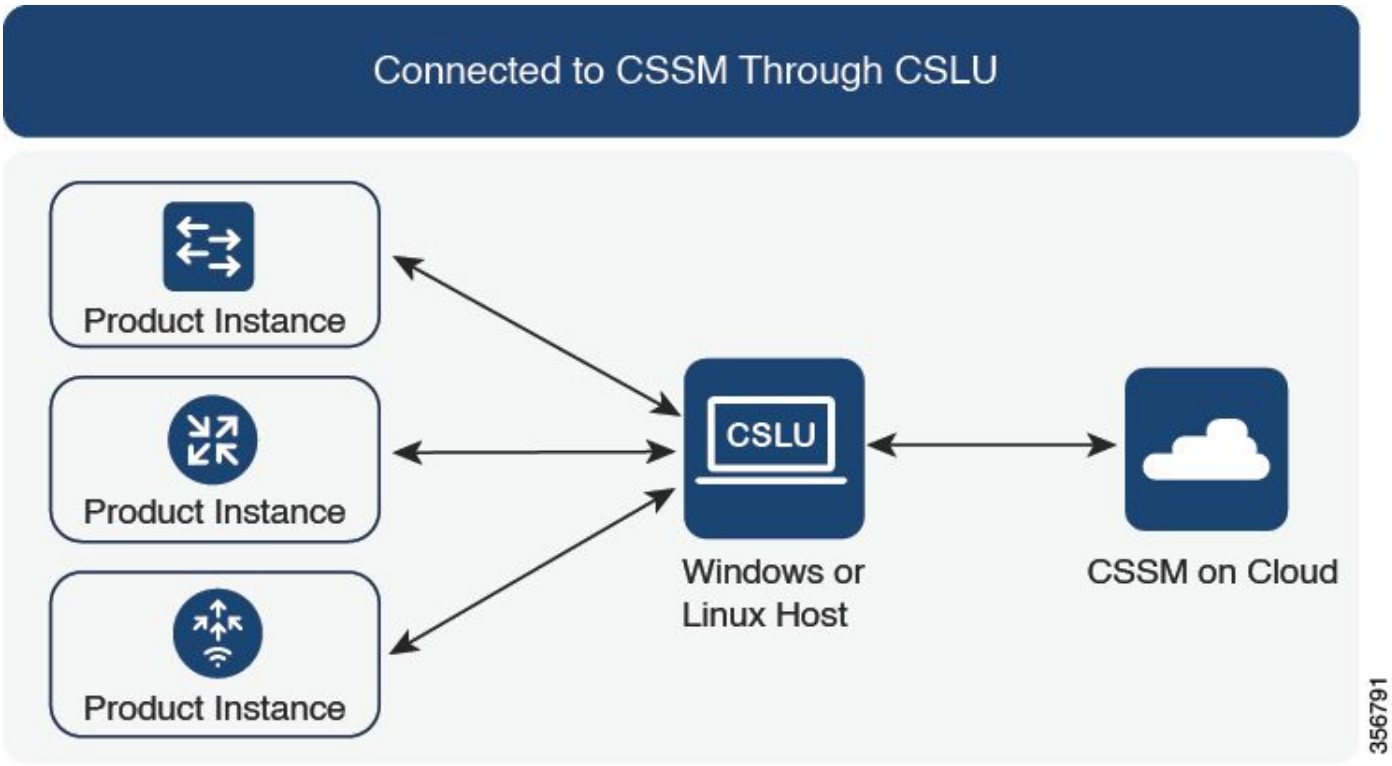
このドキュメントの情報は、17.3.2以降のCisco IOS XEデバイスに基づくものです。

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。

背景説明

この問題には、Cisco Smart Software Manager(CSSM)、Cisco Smart License Utility(CSLU)、またはCisco Smart Software Manager(SSM)オンプレミスとのスマートライセンス通信の失敗が含まれます。 Smart Licensing Using Policy(SLP)は、Smart Licensingの拡張版です。ハードウェアおよびソフトウェアライセンスのコンプライアンスを確保しながら、ネットワーク運用を中断しないライセンスソリューションを提供することを目的としています。SLPは、Cisco IOS XE Amsterdam 17.3.2以降でサポートされています。

トポロジ



CSLUを介してCSSMに接続

SLPの概要

SLPでは、以前の評価モード、登録、および予約の概念が取り除かれています。代わりに、ライセンスの使用状況の報告に重点を置いています。ライセンスは適用されず、ライセンスレベルは同じままです。SLPの主な変更点は、ライセンスの使用状況のレポートとトラッキングです。このセクションでは、SLPで導入された用語、変更の理由、および新しいコンポーネントについて説明します。

確認された問題

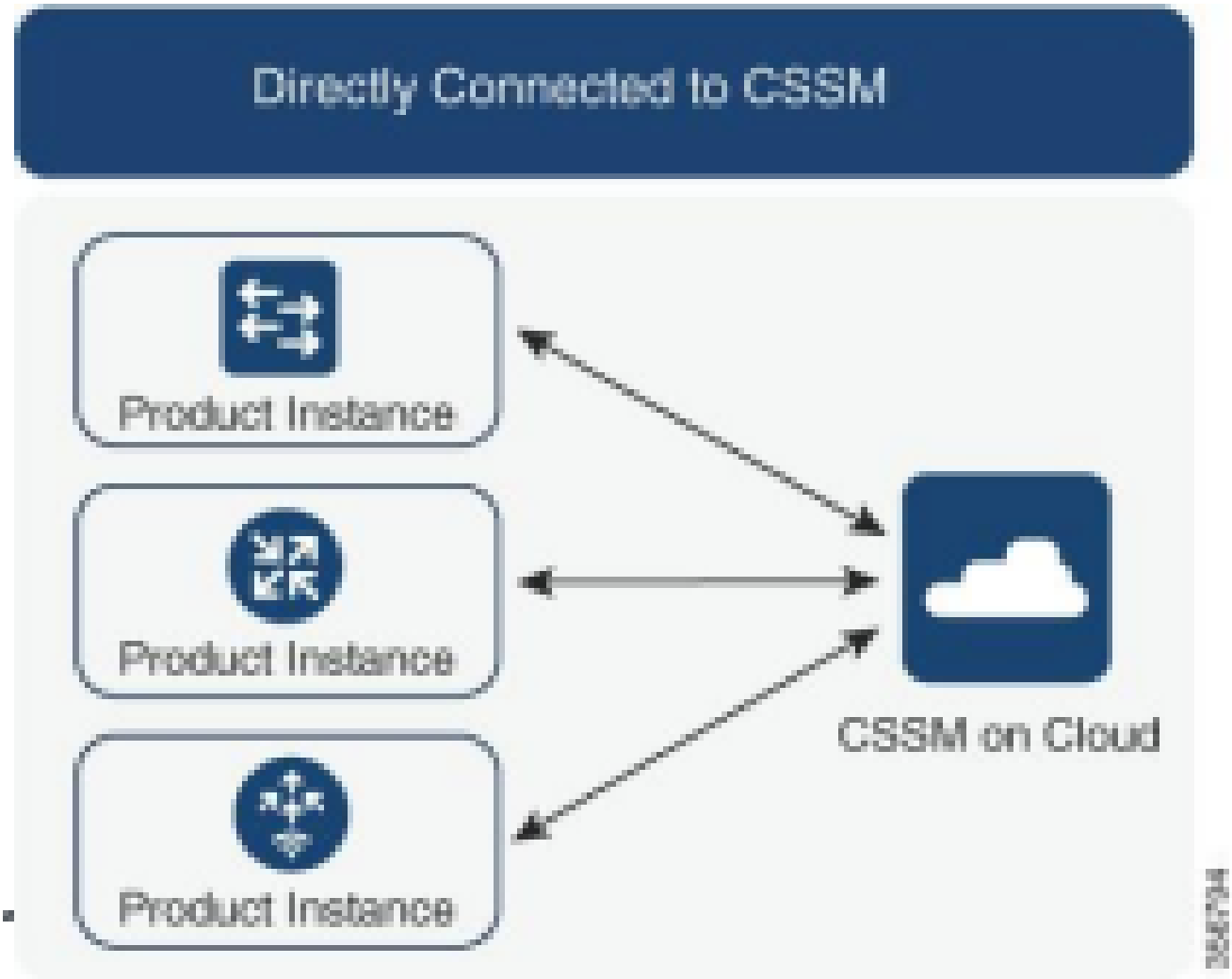
Cat9kスイッチを最新のCisco IOS 17.3.2以降にアップグレードすると、CSSM、CSLU、またはSSMのオンプレミスとのSmart Licensing通信が失敗します。

```
Error Message: %SMART_LIC-3-COMM_FAILED: Communications failure with the [chars]: [chars]
```

考えられる理由：ネットワークの到達可能性の問題またはCSSMサーバのダウンが原因で障害が発生した可能性があります。

修復手順

トポロジ



CSSMに直接接続

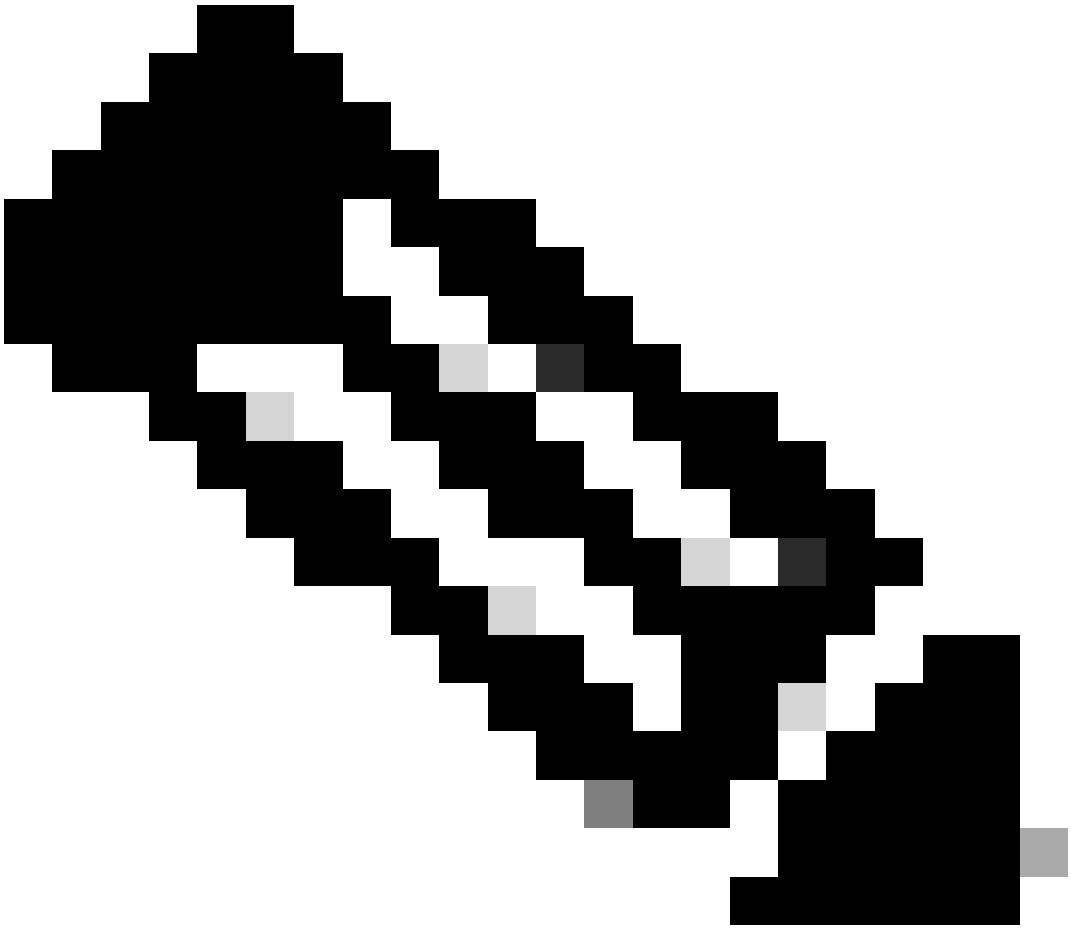
必要な手順

ステップ 1：CSSMへの到達可能性の確認

ポリシー（Cisco IOS XE 17.3.2以降）を使用したスマートライセンスをサポートするスイッチでCSSMへの直接接続を使用する場合、次の手順を実行すると、ポータルとの接続を確立してライセンスを取得できます。
1. スイッチがシスコライセンスサーバにアクセスできることを確認します。

```
Switch#ping smartreceiver.cisco.com
Switch#telnet smartreceiver.cisco.com 443
```

デバイスからCSSMへのping到達可能性



注：リファレンスセクションのCisco Liveドキュメントを参照してください。

---

2. ドメイン名でサーバに到達できない場合は、DNSスタティックエントリを設定できます。次に

例を示します。

```
Switch(config)#ip host smartreceiver.cisco.com 72.163.10.105
```

DNSスタティックエントリの設定

3. smartreceiver.cisco.comのIPアドレスを取得するには、nslookupまたは同様のユーティリティを使用します。現在ロード中です

次のIPアドレスのバランス：

smartreceiver.cisco.comのIPアドレス

ステップ 2：スイッチでのスマートトランスポートの設定

1. オートコール転送は、引き続きSLPに使用できます。ただし、これは従来の方法であり、代わりにスマートトランスポートを使用することをお勧めします。

```
Switch(config)# license smart transport smart
Switch(config)# license smart url default
```

スマートトランスポートの設定

2. CSSMとの通信が特定のVRFで発生する場合、必要に応じて特定の送信元インターフェイスを割り当てます。

```
Switch(config)# ip http client source-interface <INTERFACE-TYPE-NUMBER
```

VRFへの特定の送信元インターフェイスの割り当て

3. インターネット到達可能性のためにプロキシを使用している場合は、次のコマンドを設定してください。

```
Switch(config)# license smart proxy address "IP-ADDRESS"
Switch(config)# license smart proxy port <PORT-NUMBER>
```

インターネット到達可能性のプロキシの設定

ステップ 3：CSSMポータルからのトークンの取得

に移動します。software.cisco.com > Smart Software Manager > Manage Licenses次に、適切な仮想アカウントを選Inventory .Then, 択し、 Generalを選択します。

ステップ 4：CSSMとの信頼の確立

スイッチは、CSSMの仮想アカウントから取得したトークンを使用して、CSSMとの信頼を確立する必要があります。

```
Switch# license smart trust idtoken <TOKEN> all force
After a few minutes at the very bottom of the 'show license status'
output you should see the trust code was installed
Switch#show license status
<...>
Trust Code Installed: Feb 25 18:37:51 2021 UTC
```

トークンを使用したCSSMとの信頼の確立

ステップ 5：ライセンス使用状況レポートのトリガー

show license statusの出力が数分後に、Last report pushおよびLast ACK receivedのタイムスタンプが表示されます。

```
Switch#show license status
<...>
Usage Reporting:
  Last ACK received: Mar 27 22:33:28 2021 UTC
  Next ACK deadline: Jun 25 22:33:28 2021 UTC
  Reporting push interval: 30  days
  Next ACK push check: <none>
  Next report push: Apr 26 22:29:28 2021 UTC
  Last report push: Mar 27 22:29:28 2021 UTC
  Last report file write: <none>
```

ライセンスのステータスを確認する

CSSMに到達できない場合のトラブルシューティング手順

CSSMに到達できず、設定されているトランスポートタイプが「スマート」な場合は、次の手順を実行します。

17.3.2以降でのポリシー更新後

1. 特権EXECモードでコマンドshow license statusを使用して、スマートURLの設定を確認します。

URLが正しく「https://smartreceiver.cisco.com/licservice/license」に設定されていることを確認します。

2. 「smartreceiver.cisco.com」をpingするか、pingコマンドを使用して変換されたIPアドレスをpingして、DNS解決を確認します。例： ping

旧バージョンの場合

1. pingコマンドを使用して「**tools.cisco.com**」または変換されたIPアドレスにpingを実行し、DNS解決を確認します。例： ping tools.cisco.com
2. 製品インスタンスが正しく設定されているかどうか、および製品インスタンスのIPネットワークが稼働しているかどうかを確認します。インターフェイスコンフィギュレーションモードでno shutdownコマンドを使用して、インターフェイスコンフィギュレーションがシャットダウンされていないことを確認します。
3. デバイスにサブネットマスクとDNS IPが設定されているかどうかを確認します。
4. 特権EXECモードでコマンドshow ip http clientを使用して、HTTPSクライアントの送信元インターフェイスが正しいことを確認します。必要な場合は、グローバルコンフィギュレーションモードでip http client source-interfaceコマンドを使用して再設定します。
5. これらの手順で問題が解決しない場合は、ルーティングルールとファイアウォールの設定を再確認します。

推奨される対処法

トラブルシューティングの手順に基づいて、次の推奨処置を実行してください。

- CSSM通信用に正しいスマートURLが設定されていることを確認します。
- tools.cisco.com or smartreceiver.cisco.comのDNS解決を確認する
- 製品インスタンスとインターフェイス設定のネットワーク接続を確認します。
- サブネットマスクとDNS IP設定を確認します。
- 必要に応じて、HTTPSクライアントの送信元インターフェイスを再設定します。

すべての設定が失敗した場合は、ルーティングルールとファイアウォールの設定を確認します。

結論

このドキュメントでは、SLPの概要を説明し、Catalyst 9300スイッチをCisco IOS XE 17.3.2にアップグレードした後にユーザが直面する問題を取り上げます。CSSM、CSLU、およびSSMのオンプレミス通信障害のトラブルシューティング手順と、問題を解決するための推奨アクションが示されています。

推奨されるアクションとトラブルシューティングの手順を使用して、スマートライセンスの登録エラーを解決し、CSSM、CSLU、またはSSMオンプレミスとの正常な通信を確立できます。

関連情報

- ポリシーの更新を使用したスマートライセンス
- シスコのテクニカルサポートとダウンロード

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。