DNA Center for SWIMのHTTPSエラーのトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[問題](#)

[検証](#)

- [Cisco DNA Centerインベントリのネットワークデバイスのステータス](#)
- [ネットワークデバイスにインストールされたDNAC-CA証明書](#)

[トラブルシューティング](#)

- [ネットワークデバイスからネットワークデバイス内のCisco DNA Centerへのポート443経由の通信](#)
- [ネットワークデバイスのHTTPSクライアントソースインターフェイス](#)
- [日付の同期](#)
- [デバッグ](#)

はじめに

このドキュメントでは、Cisco IOS® XEプラットフォームのCisco DNA Center(CDNA)のSWIMプロセスにおけるHTTPSプロトコルの問題をトラブルシューティングする手順について説明します。

前提条件

要件

ADMIN ROLE権限とスイッチCLIを使用して、GUIからCisco DNA Centerにアクセスする必要があります。

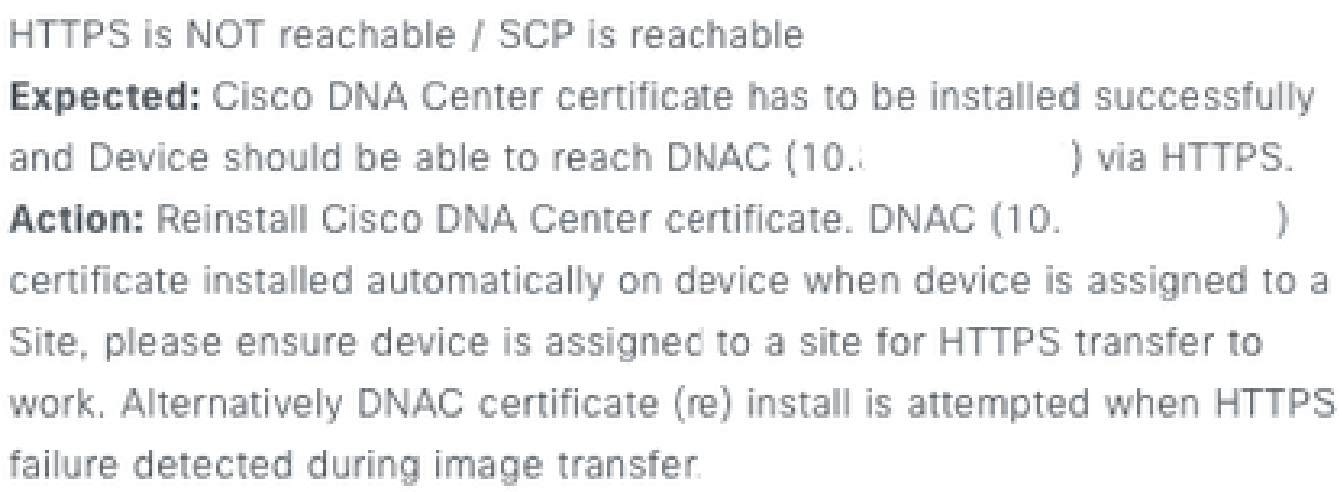
使用するコンポーネント

このドキュメントの情報は、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。

問題

Image Update Readiness Checkの後に、Cisco DNA Center(CDNA)またはSoftware Image Management(SWIM)で次のような一般的なエラーが表示されます。

「HTTPSに到達できない/SCPに到達できる」



このエラーは、HTTPSプロトコルに到達できないことを示していますが、Cisco DNA CenterはSCPプロトコルを使用してCisco IOS® XEイメージをネットワークデバイスに転送します。

SCPを使用する際の欠点の1つは、イメージの配布時間です。HTTPSはSCPよりも高速です。

検証

Cisco DNA Centerインベントリのネットワークデバイスのステータス

Provision > Inventory > Change Focus to Inventoryに移動します。

アップグレードするネットワークデバイスの到達可能性と管理性を確認します。デバイスのステータスはReachableおよびManagedである必要があります。

ネットワークデバイスの到達可能性と管理性に関するその他のステータスがある場合は、次の手順に進む前に問題を修正します。

ネットワークデバイスにインストールされたDNAC-CA証明書

ネットワークデバイスに移動し、次のコマンドを実行します。

```
show running-config | sec crypto pki
```

DNAC-CAトラストポイントとDNAC-CAチェーンが表示されている必要があります。DNAC-CAトラストポイント、チェーン、またはその両方が表示されない場合は、DNAC-CA証明書をプッシュするために「テレメトリ設定の更新」を実行する必要があります。

デバイス制御がディセーブルになっている場合は、次の手順でDNAC-CA証明書を手動でインストールします。

- Webブラウザでhttps://<dnac_ipaddress>/ca/pemandと入力し、.pemファイルをダウンロードします
- ローカルコンピュータに.pemファイルを保存します
- テキストエディタアプリケーションで.pemファイルを開く
- ネットワークデバイスのCLIを開く
- コマンドを使用して、古いDNA-CA証明書を確認します show run | in crypto pki trustpoint DNAC-CA

    - 古いDNA-CA証明書がある場合は、コンフィギュレーションモードで no crypto pki trustpoint DNAC-CA コマンドを使用してDNA-CA証明書を削除します

    - DNAC-CA証明書をインストールするには、コンフィギュレーションモードで次のコマンドを実行します。

```
crypto pki trustpoint DNAC-CA
enrollment mode ra
enrollment terminal
usage ssl-client
revocation-check none
exit
crypto pki authenticate DNAC-CA
```

    - .pemテキストファイルを貼り付けます

    - プロンプトが表示されたら、yesと入力します

    - 設定の保存

トラブルシューティング

ネットワークデバイスからネットワークデバイス内のCisco DNA Centerへのポート443経由の通信

ネットワークデバイスでHTTPSファイル転送テストを実行します

```
copy https://<DNAC_IP>/core/img/cisco-bridge.png flash:
```

このテストでは、PNGファイルをCisco DNA Centerからスイッチに転送します。

次の出力は、ファイル転送が成功したことを示しています

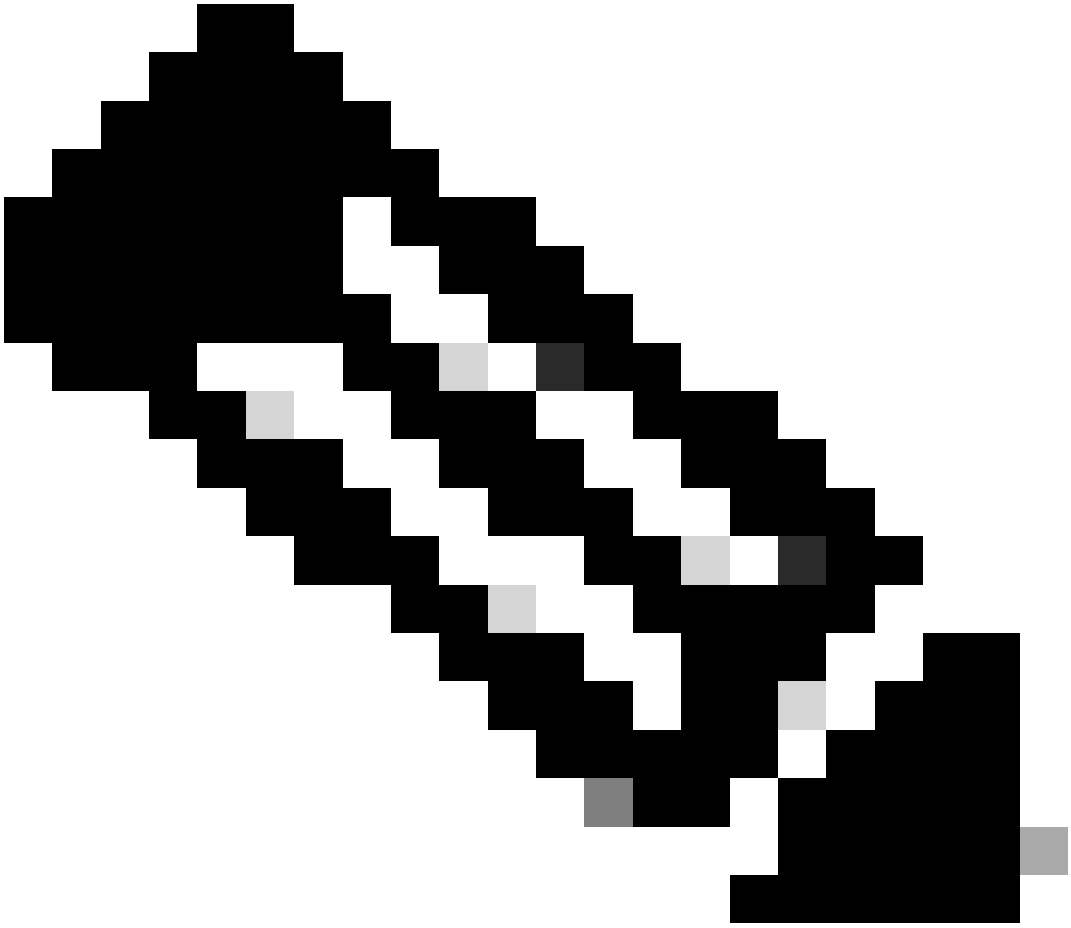
```
MXC.TAC.M.03-1001X-01#copy https://10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
Loading https://10.x.x.x/core/img/cisco-bridge.png
4058 bytes copied in 0.119 secs (34101 bytes/sec)
MXC.TAC.M.03-1001X-01#
```

次の出力が表示された場合、ファイル転送が失敗しています。

```
MXC.TAC.M.03-1001X-01#$//10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
%Error opening https://10.x.x.x/core/img/cisco-bridge.png (I/O error)
MXC.TAC.M.03-1001X-01#
```

次のアクションを実行します。

- ファイアウォールがポート443、80、および22をブロックしているかどうかを確認します。
- ネットワークデバイスに、ポート443またはHTTPSプロトコルをブロックするアクセスリストがあるかどうかを確認します。
- ファイル転送が行われている間に、ネットワークデバイスへのパケットキャプチャを実行します。



注:HTTPSファイル転送のテストが終了したら、cisco-bridge.pngファイルをコマンドで削除します delete flash:cisco-bridge.png

---

ネットワークデバイスのHTTPSクライアントソースインターフェイス

ネットワークデバイスで、クライアントソースインターフェイスが正しく設定されていることを確認します。

show run | in http client source-interface コマンドを実行すると、設定を検証できます。

MXC.TAC.M.03-1001X-01#show run | in http client source-interface

ip http client source-interface GigabitEthernet0
MXC.TAC.M.03-1001X-01#

デバイスに誤った送信元インターフェイスがある場合、または送信元インターフェイスがない場合、HTTPS転送ファイルテストは失敗します。

次の例を参照してください。

Inventory Cisco DNA CenterのラボデバイスのIPアドレスは10.88.174.43です。

インベントリのスクリーンショット：

Device Name	IP Address	Device Family	Reachability	EoX Status	Manageability
MXC.TAC.M.03-1001X-01.etlecuit.mx	10.88.174.43	Routers	Reachable	Not Scanned	Managed

HTTPSファイル転送テストに失敗しました：

MXC.TAC.M.03-1001X-01#copy https://10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
%Error opening https://10.x.x.x/core/img/cisco-bridge.png (I/O error)
MXC.TAC.M.03-1001X-01#

送信元インターフェイスを確認します。

<#root>

MXC.TAC.M.03-1001X-01#show run | in source-interface
ip ftp source-interface GigabitEthernet0

ip http client source-interface GigabitEthernet0/0/0

ip tftp source-interface GigabitEthernet0
ip ssh source-interface GigabitEthernet0
logging source-interface GigabitEthernet0 vrf Mgmt-intf

インターフェイスを確認します。

MXC.TAC.M.03-1001X-01#show ip int br | ex unassigned
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 1.x.x.x YES manual up up

GigabitEthernet0 10.88.174.43 YES TFTP up up

MXC.TAC.M.03-1001X-01#

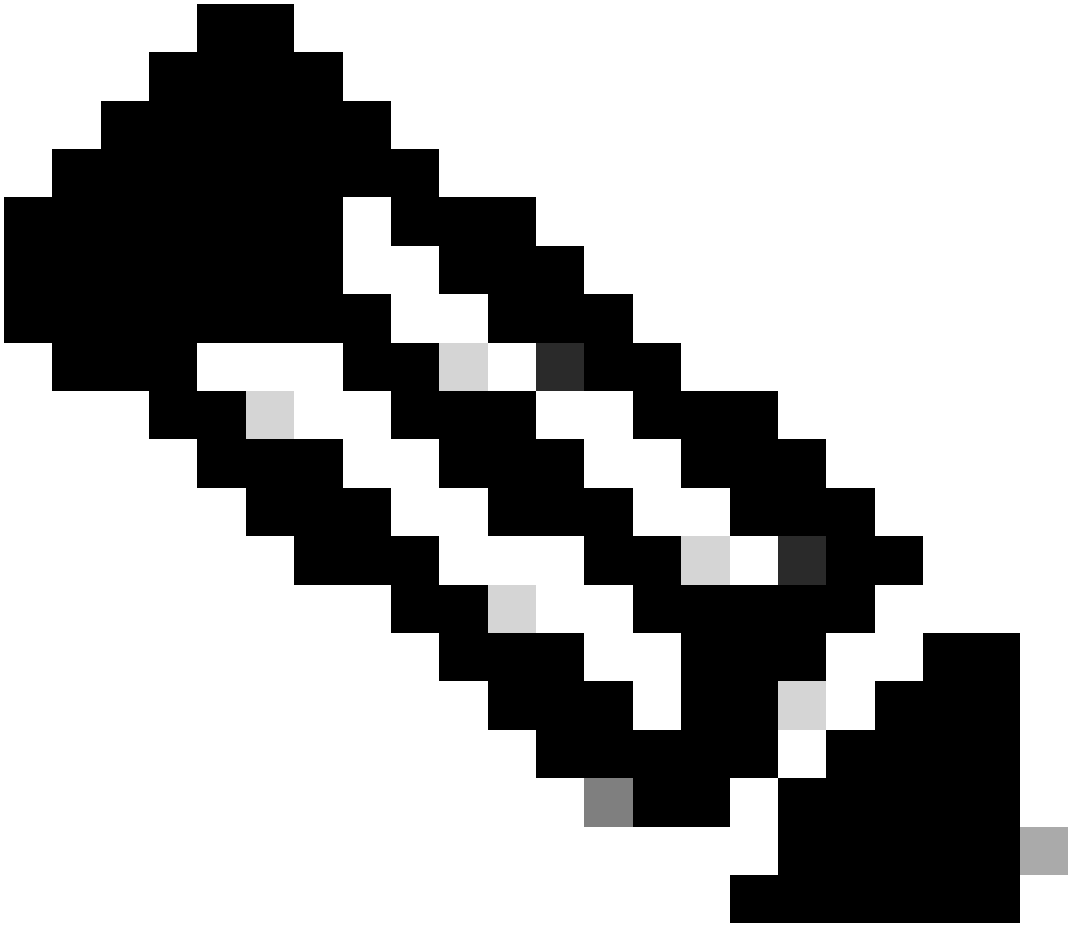
インベントリのスクリーンショットによると、Cisco DNA CenterはGigabiEthernet0/0/0ではなくGigabitEthernet0インターフェイスを使用してデバイスを検出しました

この問題を解決するには、正しい送信元インターフェイスを使用して変更する必要があります。

MXC.TAC.M.03-1001X-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MXC.TAC.M.03-1001X-0(config)#ip http client source-interface GigabitEthernet0
MXC.TAC.M.03-1001X-0(config)#

MXC.TAC.M.03-1001X-01#show run | in source-interface
ip ftp source-interface GigabitEthernet0
ip http client source-interface GigabitEthernet0
ip tftp source-interface GigabitEthernet0
ip ssh source-interface GigabitEthernet0
logging source-interface GigabitEthernet0 vrf Mgmt-intf
MXC.TAC.M.03-1001X-01#

MXC.TAC.M.03-1001X-01#copy https://10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
Loading https://10.x.x.x/core/img/cisco-bridge.png
4058 bytes copied in 0.126 secs (32206 bytes/sec)
MXC.TAC.M.03-1001X-01#



注:HTTPSファイル転送のテストが終了したら、cisco-bridge.pngファイルをコマンドで削除します delete flash:cisco-bridge.png

---

日付の同期

コマンドを使用して、ネットワークデバイスの日付とクロックが正しいことを確認します show clock

ラボデバイスでDNAC-CA証明書が欠落しているラボシナリオを参照してください。テレメトリの更新がプッシュされましたが、DNAC-CA証明書のインストールが次の理由で失敗しました：

Jan 1 10:18:05.147: CRYPTO_PKI: trustpoint DNAC-CA authentication status = 0
%CRYPTO_PKI: Cert not yet valid or is expired -
start date: 01:42:22 UTC May 26 2023
end date: 01:42:22 UTC May 25 2025

証明書は有効ですが、証明書がまだ有効でないか、期限が切れていることが工ラーで示されていることがわかります。

ネットワークデバイスの時刻を確認します。

MXC.TAC.M.03-1001X-01#show clock
10:24:20.125 UTC Sat Jan 1 1994
MXC.TAC.M.03-1001X-01#

日付と時刻に工ラーがあります。この問題を修正するには、特権モードでコマンドclock set を使用して、ntpサーバを設定するか、クロックを手動で設定します。

手動クロック設定の例：

MXC.TAC.M.03-1001X-01#clock set 16:20:00 25 september 2023

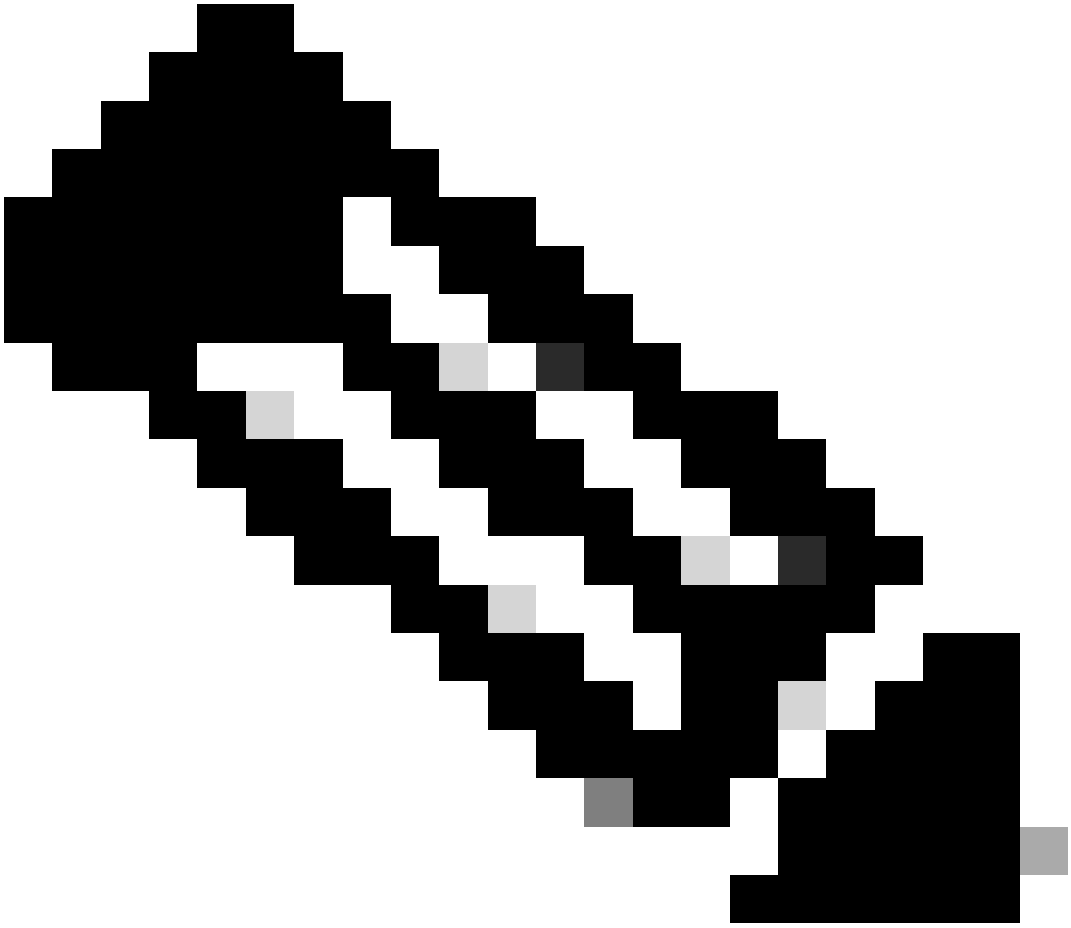
NTPの設定例：

MXC.TAC.M.03-1001X-0(config)#ntp server vrf Mgmt-intf 10.81.254.131

デバッグ

デバッグを実行して、HTTPSの問題をトラブルシューティングできます。

debug ip http all
debug crypto pki transactions
debug crypto pki validation
debug ssl openssl errors



注：ネットワークデバイスのトラブルシューティングを終了したら、次のコマンドでデバッグを停止します undebug all

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。