HTTPS-Fehler in DNA Center für SWIM beheben

Inhalt

Einleitung

In diesem Dokument wird ein Verfahren zur Fehlerbehebung bei Problemen mit dem HTTPS-Protokoll im SWIM-Prozess für Cisco DNA Center auf Cisco IOS® XE-Plattformen beschrieben.

Voraussetzungen

Anforderungen

Sie müssen über die Benutzeroberfläche mit der Berechtigung "ADMIN ROLE" und Switch CLI auf Cisco DNA Center zugreifen können.

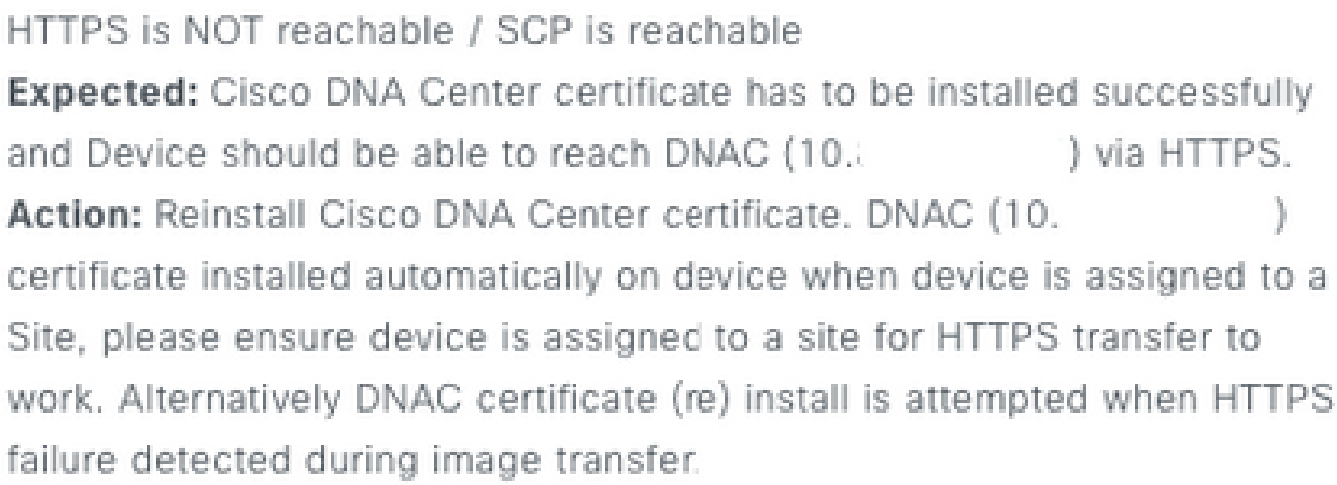
Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Problem

Es gibt einen häufigen Fehler, den Cisco DNA Center / Software Image Management (SWIM) nach der Image Update Readiness Check anzeigt:

"HTTPS ist NICHT erreichbar/SCP ist erreichbar"



Dieser Fehler beschreibt, dass das HTTPS-Protokoll nicht erreichbar ist. Cisco DNA Center verwendet jedoch das SCP-Protokoll, um das Cisco IOS® XE-Image auf das Netzwerkgerät zu übertragen.

Ein Nachteil bei der Verwendung von SCP ist die Zeitdauer für die Verteilung des Bildes. HTTPS ist schneller als SCP.

Verifizierung

Status der Netzwerkgeräte im Cisco DNA Center-Bestand

Navigieren Sie zu Provisionierung > Bestand > Fokus in Bestand ändern.

Überprüfen der Erreichbarkeit und Verwaltbarkeit des Netzwerkgeräts, das aktualisiert werden soll Der Status des Geräts muss Reachable (Erreichbar) und Managed (Verwaltet) lauten.

Wenn das Netzwerkgerät einen anderen Status in Erreichbarkeit und Verwaltbarkeit aufweist, beheben Sie das Problem, bevor Sie mit den nächsten Schritten fortfahren.

DNAC-CA-Zertifikat auf Netzwerkgerät installiert

Rufen Sie das Netzwerkgerät auf, und führen Sie den folgenden Befehl aus:

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

Sie müssen DNAC-CA Trustpoint und DNAC-CA Chain sehen. Wenn der DNAC-CA-Vertrauenspunkt, die Kette oder beides nicht angezeigt wird, müssen Sie die Telemetrieeinstellungen aktualisieren, um das DNAC-CA-Zertifikat zu übertragen.

Wenn die Gerätesteuerbarkeit deaktiviert ist, installieren Sie das DNAC-CA-Zertifikat manuell mit den folgenden Schritten:

- Geben Sie in einem Webbrowser https://<dnac_ipaddress>/ca/pdemand ein, um die .pem-Datei herunterzuladen.
- Speichern Sie die .pem-Datei auf Ihrem lokalen Computer.
- Öffnen einer .pem-Datei mit einer Texteditoranwendung
- Öffnen der CLI des Netzwerkgeräts
- Überprüfen Sie mit dem folgenden Befehl alle alten DNA-CA-Zertifikate show run | in crypto pki trustpoint DNAC-CA

    - Wenn ein altes DNA-CA-Zertifikat vorhanden ist, entfernen Sie DNAC-CA cert mit dem Befehl no crypto pki trustpoint DNAC-CA im Konfigurationsmodus.

    - Führen Sie die Befehle im Konfigurationsmodus aus, um das DNAC-CA-Zertifikat zu installieren:

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

    - Einfügen der .pem-Textdatei

    - Geben Sie yes ein, wenn Sie dazu aufgefordert werden

    - Speichern Sie die Konfiguration.

Fehlerbehebung

Kommunikation vom Netzwerkgerät zum Cisco DNA Center im Netzwerkgerät über Port 443

Führen Sie den HTTPS-Dateiübertragungstest auf Ihrem Netzwerkgerät aus.

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

Bei diesem Test wird eine PNG-Datei vom Cisco DNA Center an den Switch übertragen.

Diese Ausgabe beschreibt die erfolgreiche Dateiübertragung.

```
MXC.TAC.M.03-1001X-01#copy https://10.x.x.x/core/img/cisco-bridge.png flash:
```

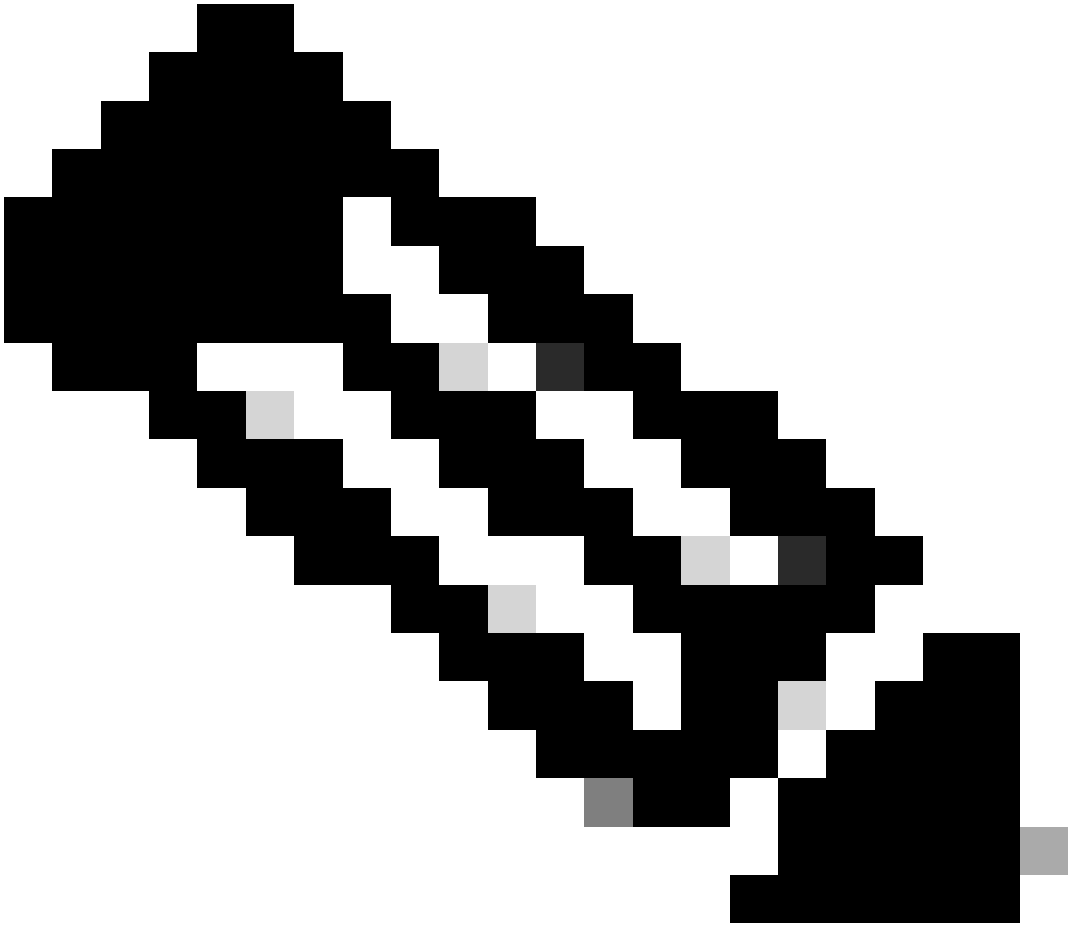
Destination filename [cisco-bridge.png]?
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
Loading https://10.x.x.x/core/img/cisco-bridge.png
4058 bytes copied in 0.119 secs (34101 bytes/sec)
MXC.TAC.M.03-1001X-01#

Wenn Sie die nächste Ausgabe erhalten, ist die Dateiübertragung fehlgeschlagen:

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#

Führen Sie die nächsten Schritte aus:

- Überprüfen Sie, ob die Firewall die Ports 443, 80 und 22 blockiert.
- Überprüfen Sie, ob eine Zugriffsliste im Netzwerkgerät vorhanden ist, das den Port 443 oder das HTTPS-Protokoll blockiert.
- Führen Sie während der Dateiübertragung eine Paketerfassung für das Netzwerkgerät durch.



Hinweis: Entfernen Sie die Datei cisco-bridge.png mit dem Befehl, nachdem Sie den HTTPS-Dateitransfer getestet haben. delete flash:cisco-bridge.png

---

HTTPS-Client-Quellschnittstelle in Netzwerkgerät

Überprüfen Sie, ob die Client-Quellschnittstelle des Netzwerkgeräts korrekt konfiguriert ist.

Sie können den Befehl ausführen, show run | in http client source-interface um die Konfiguration zu validieren:

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#

Der HTTPS-Dateiübertragungstest schlägt fehl, wenn das Gerät über eine falsche Quellschnittstelle verfügt oder die Quellschnittstelle fehlt.

Sehen Sie sich das Beispiel an:

Das Gerät im Labor hat die IP-Adresse 10.88.174.43 im Inventory Cisco DNA Center:

Screenshot des Bestands:

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

Fehler beim HTTPS-Dateiübertragungstest:

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#

Überprüfen der Quellschnittstelle:

<#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
```

Schnittstellen überprüfen:

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#

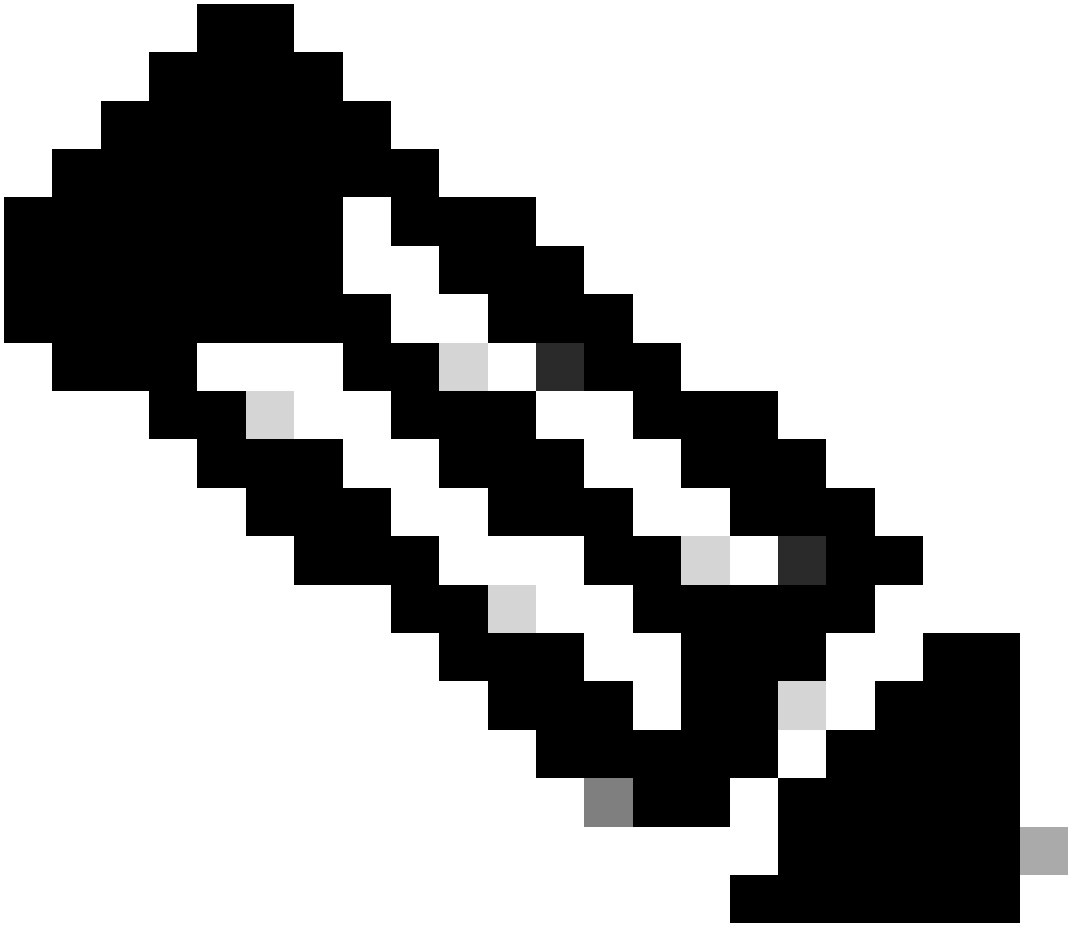
Laut Screenshot des Inventars entdeckte Cisco DNA Center das Gerät mithilfe der Schnittstelle GigabitEthernet0 anstelle von GigabiEthernet0/0/0.

Sie müssen die Änderungen mit der richtigen Quellschnittstelle vornehmen, um das Problem zu beheben.

```
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#
```



Hinweis: Entfernen Sie die Datei cisco-bridge.png mit dem Befehl, nachdem Sie den HTTPS-Dateitransfer getestet haben. delete flash:cisco-bridge.png

---

Synchronisierung

Überprüfen Sie mithilfe des Befehls, ob das Netzwerkgerät das richtige Datum und die richtige Uhrzeit aufweist. show clock

Sehen Sie sich das Laborszenario an, in dem das DNAC-CA-Zertifikat auf dem LAB-Gerät fehlte. Das Telemetrie-Update wurde angestoßen. Fehler bei der Installation des DNAC-CA-Zertifikats:

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

Wie Sie sehen, ist das Zertifikat gültig. Der Fehler besagt jedoch, dass das Zertifikat noch nicht gültig ist oder abgelaufen ist.

Zeit des Netzwerkgeräts überprüfen:

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

Bei Datum und Uhrzeit ist ein Fehler aufgetreten. Um dieses Problem zu beheben, können Sie einen NTP-Server konfigurieren oder die Uhr manuell mit dem Befehl clock set im privilegierten Modus konfigurieren.

Konfigurationsbeispiel für manuelle Uhr:

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

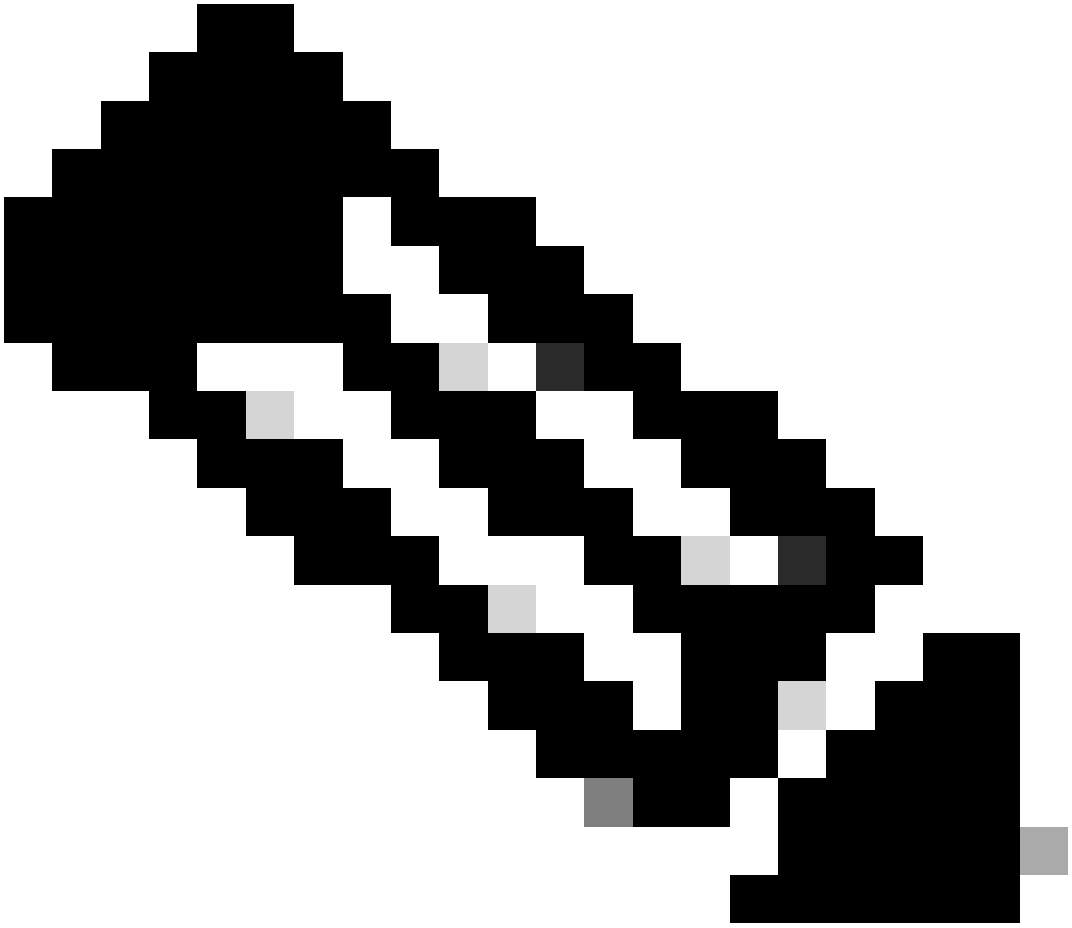
NTP-Konfigurationsbeispiel:

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

Fehlerbehebung

Sie können zur Fehlerbehebung von HTTPS-Problemen Debug-Vorgänge ausführen:

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



Hinweis: Beenden Sie die Fehlersuche mit dem Befehl, nachdem Sie die Fehlerbehebung für das Netzwerkgerät abgeschlossen haben. undebug all

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.