HTTPS-fout in DNA Center voor SWIM oplossen

Inhoud

Inleiding

Dit document beschrijft een procedure voor het oplossen van problemen met HTTPS-protocol in het SWIM-proces voor Cisco DNA Center in Cisco IOS® XE-platforms.

Voorwaarden

Vereisten

U moet toegang hebben tot Cisco DNA Center via GUI met ADMIN ROL privilege en switch CLI.

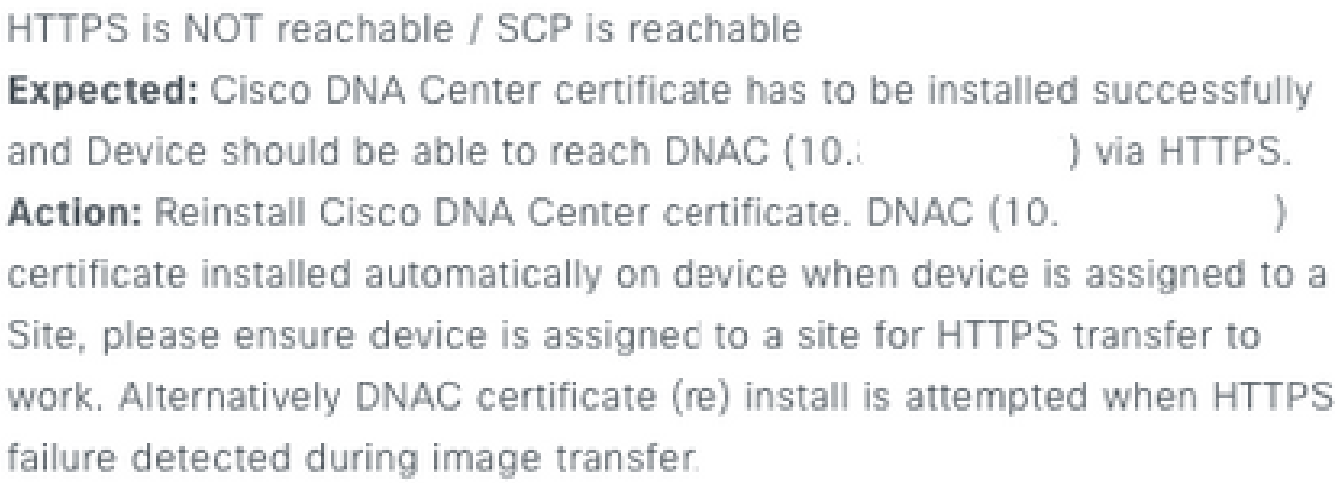
Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleem

Er is een veel voorkomende fout die wordt weergegeven door Cisco DNA Center / Software Image Management (SWIM) nadat de gereedheid voor het bijwerken van het image is gecontroleerd:

"HTTPS is NIET bereikbaar / SCP is bereikbaar"



Deze fout beschrijft dat het HTTPS-protocol niet bereikbaar is. Cisco DNA Center gaat echter het SCP-protocol gebruiken om de afbeelding van Cisco IOS® XE naar het netwerkapparaat over te dragen.

Eén nadeel voor het gebruik van SCP is de hoeveelheid tijd die nodig is om de afbeelding te distribueren. HTTPS is sneller dan SCP.

Verificatie

Status netwerkapparaat in Cisco DNA Center Inventory

Navigeer naar Voorziening > Inventaris > Focus op inventaris wijzigen

Controleer de bereikbaarheid en beheerbaarheid van het netwerkapparaat dat u wilt upgraden. De status van het apparaat moet bereikbaar en beheerd zijn.

Als het netwerkapparaat een andere status heeft op het gebied van bereikbaarheid en beheerbaarheid, kunt u het probleem oplossen voordat u naar de volgende stappen gaat.

DNAC-CA-certificaat geïnstalleerd op netwerkapparaat

Ga naar het netwerkapparaat en voer de opdracht uit:

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

U moet DNAC-CA trustpoint en DNAC-CA keten zien. Als u geen DNAC-CA trustpoint, keten of beide kunt zien, moet u de Telemetry Settings bijwerken om het DNAC-CA certificaat te kunnen doordrukken.

Als de controleerbaarheid van het apparaat is uitgeschakeld, installeer DNAC-CA certificaat handmatig met de volgende stappen:

- In een webbrowser type https://<dnac_ipaddress>/ca/pemand downloaden van het .pem-bestand
- Sla het .pem-bestand op uw lokale computer op
- Open .pem-bestand met een tekstverdelertoepassing
- CLI voor open netwerkapparaat
- Controleer elk oud DNA-CA certificaat met de opdracht show run | in crypto pki trustpoint DNAC-CA

    - Als er een oud DNA-CA certificaat is, verwijder DNAC-CA cert met de opdracht no crypto pki trustpoint DNAC-CA in configuratiemodus

    - Voer de opdrachten in de configuratiemodus uit om DNAC-CA cert te installeren:

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

    - Het tekstbestand .pem plakken

    - Voer ja in wanneer hierom wordt gevraagd

    - Sla de configuratie op

Probleemoplossing

Communicatie van netwerkapparaat naar Cisco DNA Center in netwerkapparaat via poort 443

Voer de HTTPS-test voor bestandsoverdracht uit op uw netwerkapparaat

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

Met deze test wordt een PNG-bestand van Cisco DNA Center naar de switch overgebracht.

Deze uitvoer beschrijft of de bestandsoverdracht succesvol is

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

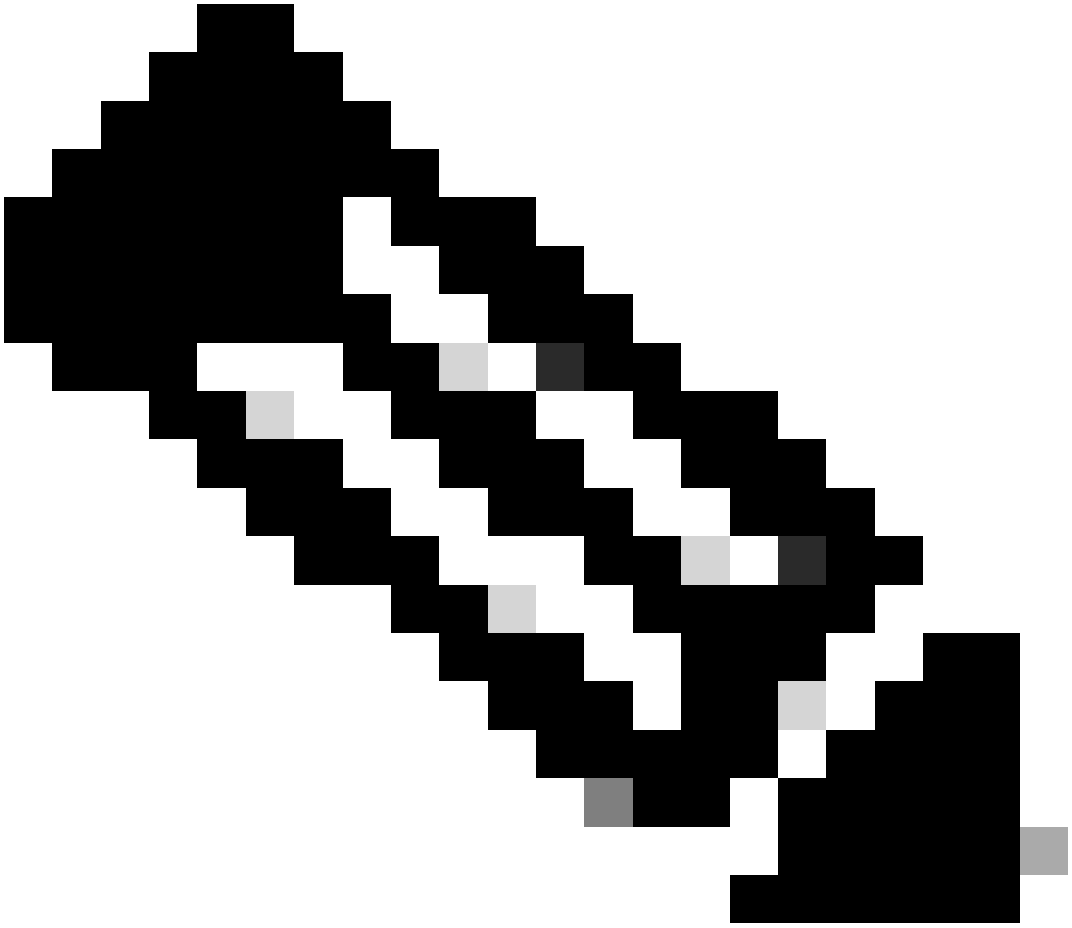
```
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
Loading https://10.x.x.x/core/img/cisco-bridge.png
4058 bytes copied in 0.119 secs (34101 bytes/sec)
MXC.TAC.M.03-1001X-01#
```

Als u de volgende uitvoer krijgt, is de bestandsoverdracht mislukt:

```
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#
```

Voer de volgende handelingen uit:

- Controleer of de firewall poort 443, 80 en 22 blokkeert.
- Controleer of er een toegangslijst is in poort 443 voor netwerkapparaten of in het HTTPS-protocol.
- Neem een pakket op in het netwerkapparaat terwijl de bestandsoverdracht plaatsvindt.



Opmerking: Nadat u klaar bent met het testen van HTTPS-bestandsoverdracht, verwijdert u het bestand cisco-bridge.png met de opdracht delete flash:cisco-bridge.png

---

HTTPS-clientbroninterface in netwerkapparaat

Controleer of de broninterface van de client op het netwerkapparaat correct is geconfigureerd.

U kunt de opdracht uitvoeren show run | in http client source-interface om de configuratie te valideren:

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#

De HTTPS-overdrachtbestandstest zal mislukken als het apparaat een onjuiste broninterface heeft of de broninterface ontbreekt.

Neem een kijkje bij het voorbeeld:

Het apparaat van het laboratorium heeft het IP adres 10.88.174.43 in het Centrum van Cisco DNA van de Inventaris:

Screenshot van de inventaris:

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-test voor bestandsoverdracht mislukt:

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#

Controleer de bron-interface:

<#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
```

Controleer interfaces:

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#

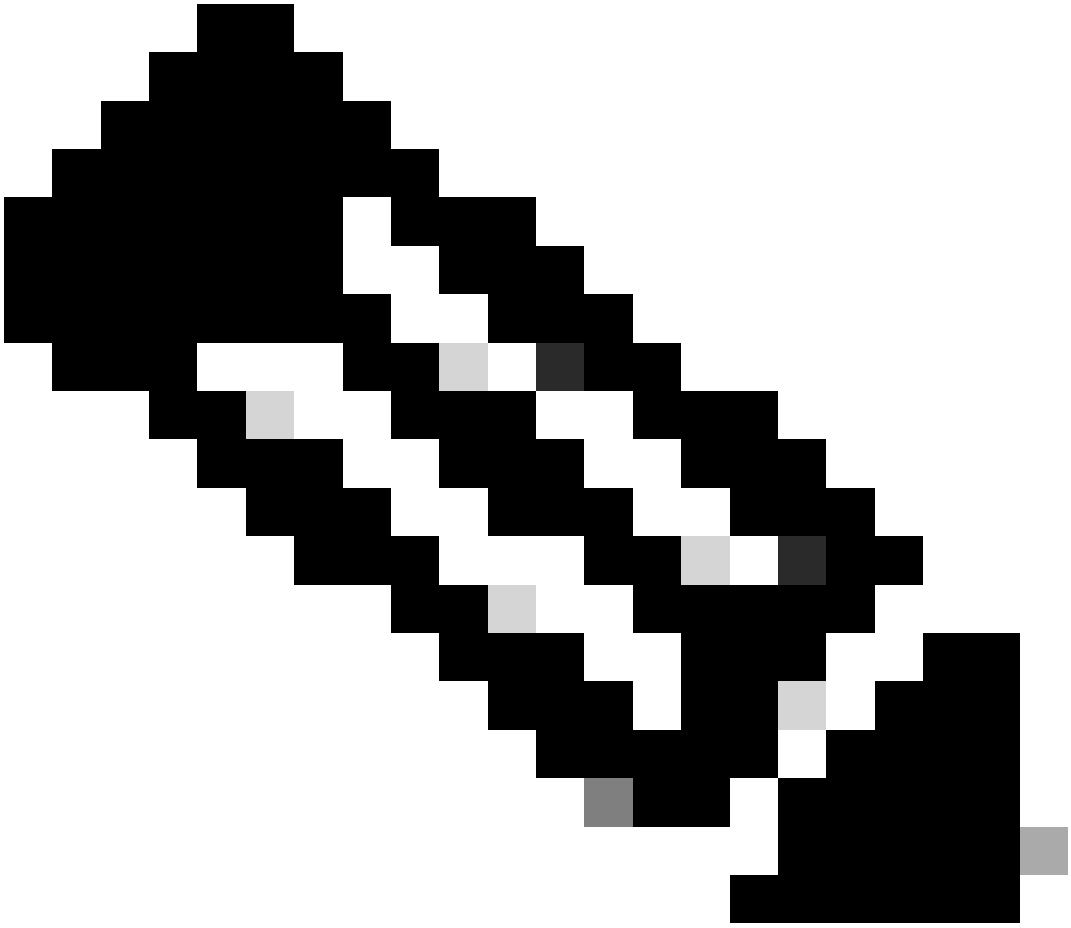
Volgens een screenshot van de inventaris, ontdekte Cisco DNA Center het apparaat met behulp van de interface Gigabit Ethernet0 in plaats van Gigabit Ethernet0/0/0

U moet zich aanpassen met de juiste broninterface om het probleem op te lossen.

```
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#
```



Opmerking: Nadat u klaar bent met het testen van HTTPS-bestandsoverdracht, verwijdert u het bestand cisco-bridge.png met de opdracht delete flash:cisco-bridge.png

---

Datumsynchronisatie

Controleer of het netwerkapparaat de juiste datum en klok heeft met de opdracht show clock

Neem een kijkje in het lab scenario waar DNAC-CA certificaat ontbrak in LAB apparaat. Het bijwerken van de telemetrie werd geduwd; nochtans, de installatie van het DNAC-CA- certificaat ontbrak wegens:

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

Zoals u kunt zien, is de cert geldig; echter, de fout zei dat cert nog niet geldig is of is verlopen.

Controleer de tijd van het netwerkapparaat:

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

Er is een fout met de datum en de tijd. Om dit probleem op te lossen, kunt u een ntp server configureren of handmatig de kloktijd configureren met de opdracht clock set in de voorkeursmodus.

Handmatig voorbeeld van klokconfiguratie:

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

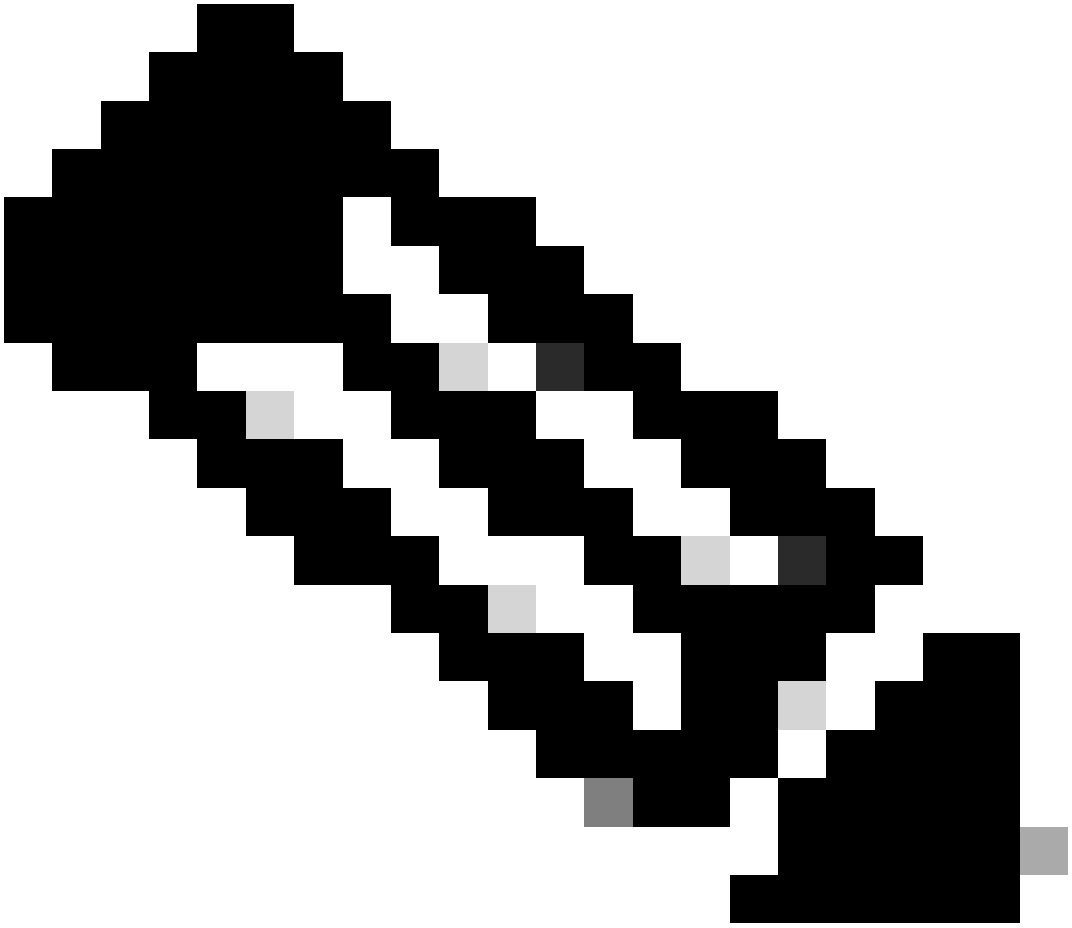
NTP-configuratievoorbeeld:

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

Debugs

U kunt debugs uitvoeren om HTTPS-probleem op te lossen:

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



Opmerking: nadat u klaar bent met het oplossen van problemen met het netwerkapparaat, stop de debugs met de opdracht undebug all

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.