排除Cisco Catalyst Center for SWIM中的HTTPS錯誤

目錄

簡介

本檔案介紹用於疑難排解Cisco IOS® XE平台Cisco Catalyst Center的SWIM程式中HTTPS通訊協定問題的程式。

必要條件

需求

您必須透過具有ADMIN ROLE許可權的GUI和交換機CLI訪問Cisco Catalyst Center。

Cisco Catalyst Center必須在物理裝置中運行。

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

Cisco Catalyst中心/軟體映像管理(SWIM)在映像更新就緒性檢查後顯示一個常見錯誤：

「HTTPS無法訪問/SCP可訪問」

HTTPS is NOT reachable / SCP is reachable

Expected: Cisco DNA Center certificate has to be installed successfully and Device should be able to reach DNAC (10.) via HTTPS.

Action: Reinstall Cisco DNA Center certificate. DNAC (10.) certificate installed automatically on device when device is assigned to a Site, please ensure device is assigned to a site for HTTPS transfer to work. Alternatively DNAC certificate (re) install is attempted when HTTPS failure detected during image transfer.

此錯誤說明HTTPS協定無法訪問；但是，Cisco Catalyst Center將使用SCP協定將Cisco IOS® XE映像傳輸到網路裝置。

使用SCP的一個缺點是分配映像的時間長。HTTPS比SCP快。

驗證

Cisco Catalyst中心資產中的網路裝置狀態

導航到調配 > 資產 >將焦點更改為資產

驗證要升級的網路裝置的可接通性和可管理性。裝置的狀態必須為可訪問和託管。

如果網路裝置處於「可接通性」和「可管理性」狀態，請先解決此問題，然後再執行後續步驟。

網路裝置中安裝的DNAC-CA證書

轉到網路裝置並運行命令：

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

您必須看到DNAC-CA信任點和DNAC-CA鏈。如果無法看到DNAC-CA信任點、鏈或兩者，則需要使用更新遙測設定以推送DNAC-CA證書。

如果停用裝置可控性，請按照以下步驟手動安裝DNAC-CA憑證：

- 在Web瀏覽器中，輸入https://<dnac_ipaddress>/ca/peand下載.pem檔案
- 將.pem檔案儲存在本機電腦中
- 使用文字編輯器應用程式開啟.pem檔案
- 打開網路裝置CLI
- 使用命令驗證任何舊的DNA-CA證書 show run | in crypto pki trustpoint DNAC-CA
    - 如果有舊的DNA-CA證書，請在配置模式下使用 no crypto pki trustpoint DNAC-CA 命令刪除DNAC-CA證書

- 在配置模式下運行命令以安裝DNAC-CA證書：

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

- 貼上.pem文字檔
- 出現提示時輸入yes
- 儲存配置

疑難排解

網路裝置透過埠443與Cisco Catalyst中心通訊

在網路裝置中運行HTTPS檔案傳輸測試

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

此測試會將PNG檔案從Cisco Catalyst Center傳輸到交換機。

此輸出說明檔案傳輸成功

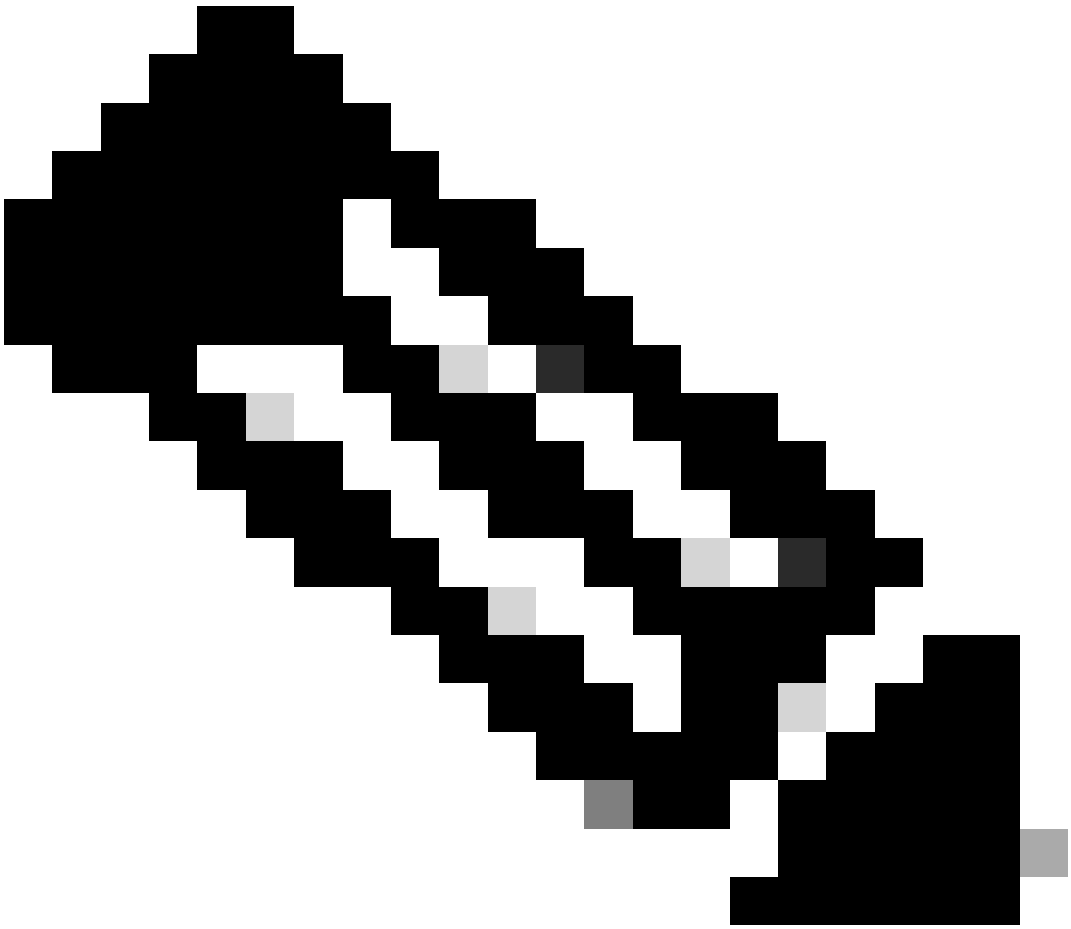
```
MXC.TAC.M.03-1001X-01#copy https://10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
Loading https://10.x.x.x/core/img/cisco-bridge.png
4058 bytes copied in 0.119 secs (34101 bytes/sec)
MXC.TAC.M.03-1001X-01#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

如果得到下一個輸出，則檔案傳輸失敗：

```
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#
```

採取以下操作：

- 驗證防火牆是否阻止埠443、80和22。
- 驗證網路裝置中是否存在阻止埠443或HTTPS協定的訪問清單。
- 進行檔案傳輸時，對網路裝置執行資料包捕獲。



注意：此產品對Cisco Catalyst虛擬裝置無效。

完成測試HTTPS檔案傳輸後，使用命令刪除cisco-bridge.png檔案 delete flash:cisco-bridge.png

---

網路裝置中的HTTPS客戶端源介面

驗證您的網路裝置客戶端源介面是否配置正確。

您可以運行命令 show run | in http client source-interface 來驗證配置：

```
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#
```

如果裝置具有不正確的源介面或缺少源介面，則HTTPS傳輸檔案測試將失敗。

請看示例：

實驗室裝置在清單Cisco Catalyst中心中的IP地址為10.88.174.43：

資產螢幕截圖：

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檔案傳輸測試失敗：

```
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#
```

驗證來源介面：

<#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
```

驗證介面：

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#

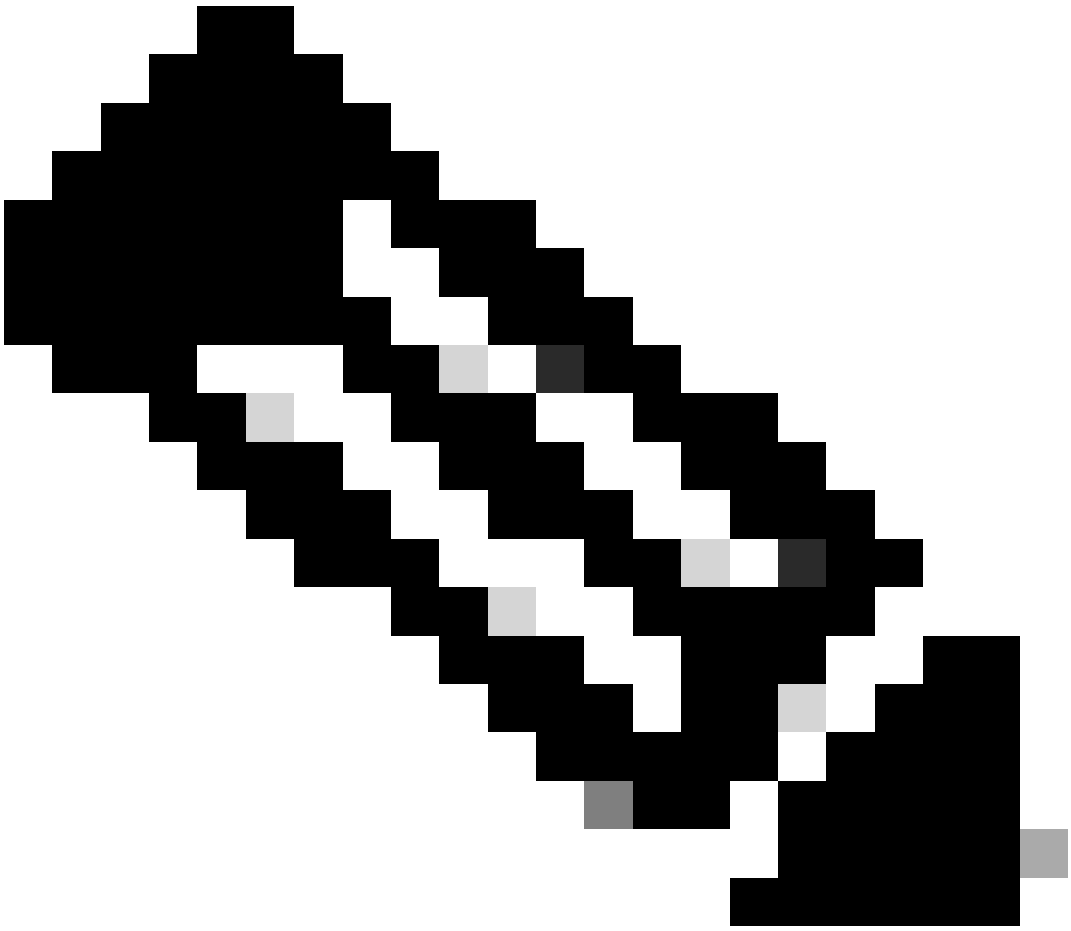
根據清單螢幕截圖，Cisco Catalyst Center發現裝置使用介面GigabitEthernet0（而不是GigabiEthernet0/0/0）

您需要使用正確的來源介面進行修改才能修正問題。

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#



注意：完成測試HTTPS檔案傳輸後，使用命令刪除cisco-bridge.png檔案 delete flash:cisco-bridge.png

---

日期同步

使用命令檢驗網路裝置是否有正確的日期和時間 show clock

瞭解實驗室裝置中缺少DNAC-CA證書的情況。已推送遙測更新；但是，DNAC-CA證書安裝失敗，原因是：

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

如您所見，證書有效；但是，錯誤表明證書尚未有效或已過期。

驗證網路裝置時間：

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

日期和時間有錯誤。要解決此問題，您可以在特權模式下配置ntp伺服器或使用命令clock set 手動配置時鐘。

手動時鐘配置示例：

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

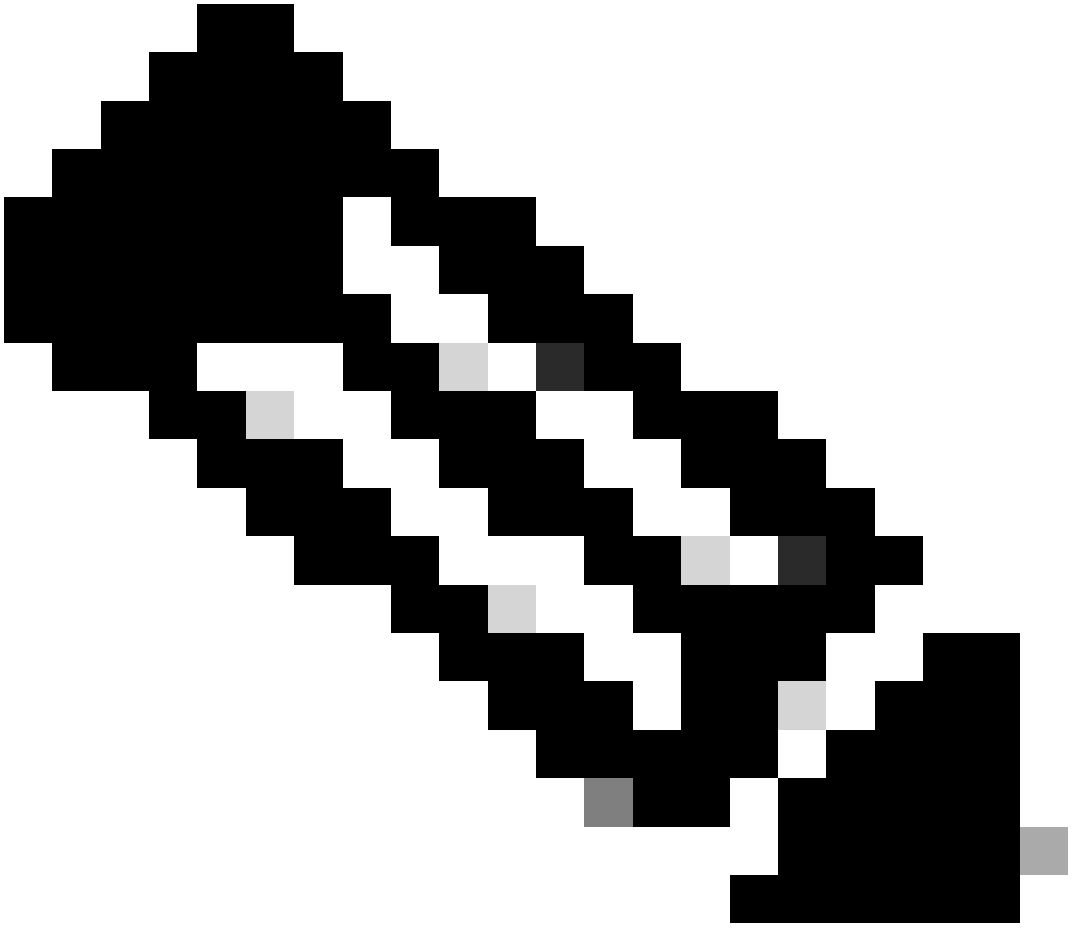
NTP**配置示例：**

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

調試

您可以執行偵錯來疑難排解HTTPS**問題：**

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



注意：完成網路裝置故障排除後，請使用命令停止調試 undebug all

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。