排除DNA Center for SWIM中的HTTPS错误

目录

简介

本文档介绍用于对Cisco IOS® XE平台中Cisco DNA中心的SWIM过程中的HTTPS协议问题进行故障排除的过程。

先决条件

要求

您必须具有管理员角色权限和交换机CLI，通过GUI访问Cisco DNA Center。

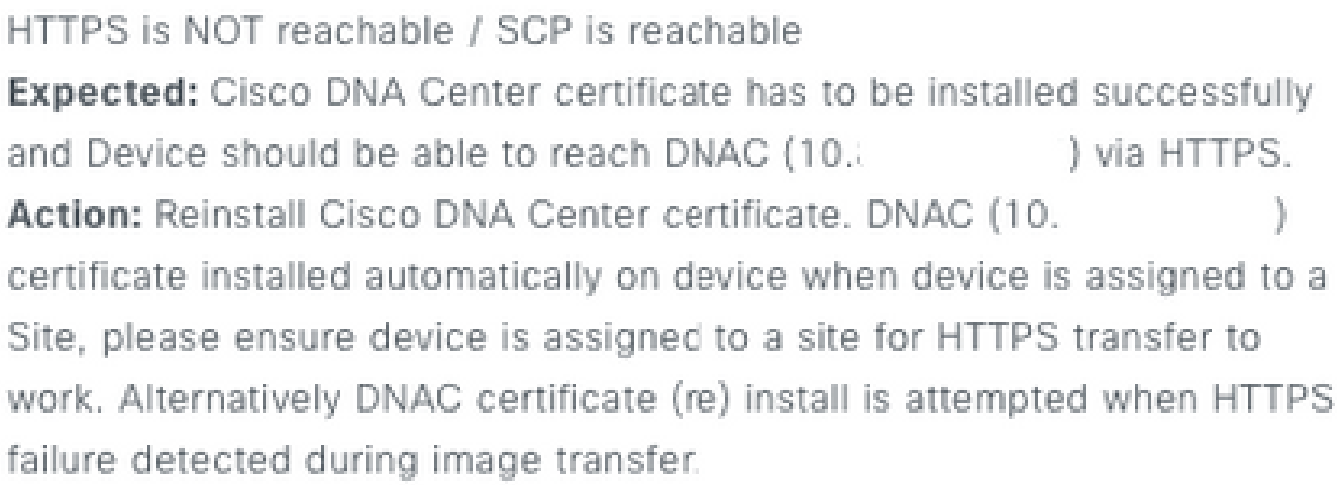
使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

Cisco DNA中心/软件映像管理(SWIM)在映像更新就绪性检查后显示一个常见错误：

“HTTPS不可达/SCP可达”



此错误描述无法访问HTTPS协议；但是，Cisco DNA中心将使用SCP协议将Cisco IOS® XE映像传输到网络设备。

使用SCP的一个缺点是分发映像的时间长。HTTPS比SCP更快。

确认

思科DNA中心资产中的网络设备状态

导航到调配 > 资产 >将重点更改为资产

验证要升级的网络设备的可接通性和可管理性。设备的状态必须为可访问和托管。

如果网络设备的连通性和可管理性处于任何其他状态，请先解决此问题，然后再继续下一步。

网络设备中安装的DNAC-CA证书

转到网络设备并运行命令：

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

您必须看到DNAC-CA信任点和DNAC-CA链。如果无法看到DNAC-CA信任点、链或两者，则需要更新遥测设置以推送DNAC-CA证书。

如果禁用设备可控性，请按照以下步骤手动安装DNAC-CA证书：

- 在Web浏览器中，键入https:// <dnac_ipaddress>/ca/pemand下载.pem文件
- 将.pem文件保存到本地计算机中
- 使用文本编辑器应用程序打开.pem文件
- 开放式网络设备CLI
- 使用命令验证任何旧的DNA-CA证书 show run | in crypto pki trustpoint DNAC-CA
    - 如果有旧的DNA-CA证书，请在配置模式下使用 no crypto pki trustpoint DNAC-CA 命令删除DNAC-CA证书

- 在配置模式下运行命令以安装DNAC-CA证书：

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

- 粘贴文本文件.pem
- 出现提示时输入yes
- 保存配置

故障排除

网络设备通过端口443与网络设备中的Cisco DNA中心通信

在网络设备上运行HTTPS文件传输测试

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

此测试将PNG文件从Cisco DNA Center传输到交换机。

此输出描述文件传输是否成功

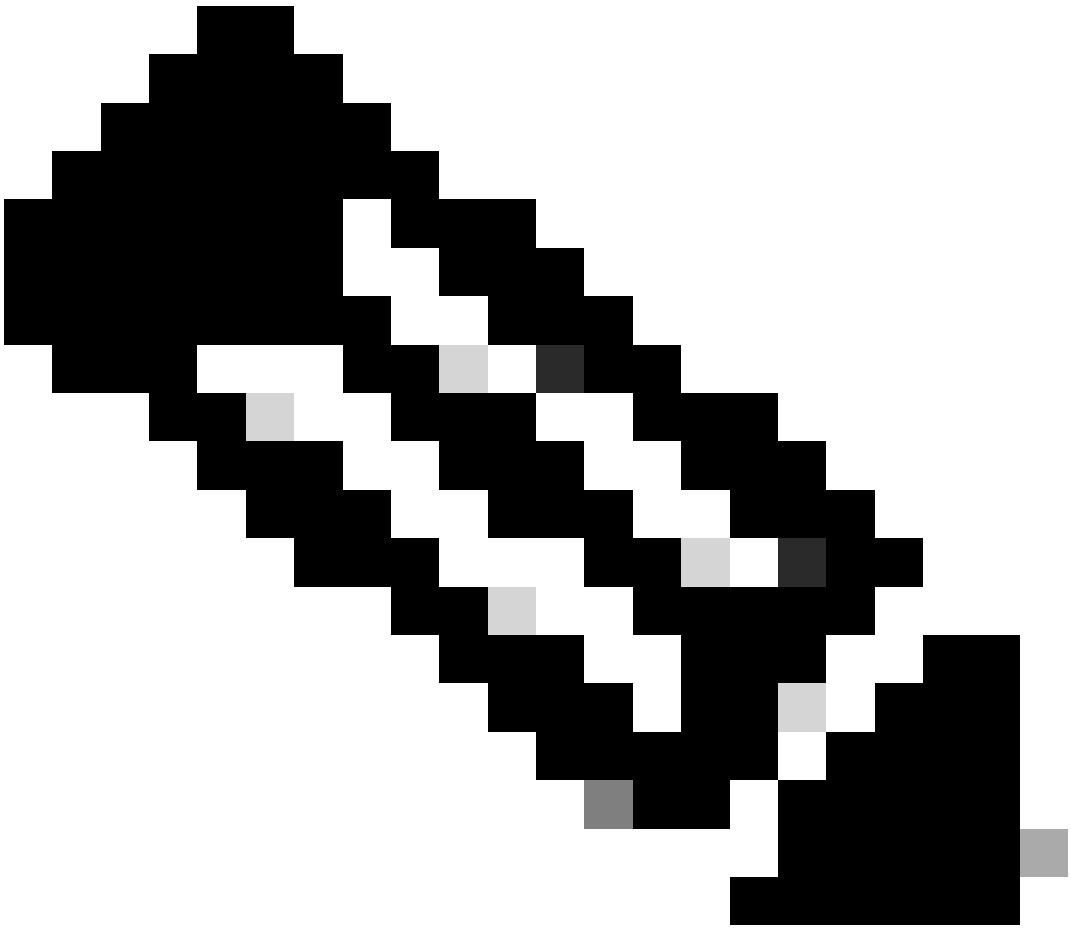
```
MXC.TAC.M.03-1001X-01#copy https://10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
Loading https://10.x.x.x/core/img/cisco-bridge.png
4058 bytes copied in 0.119 secs (34101 bytes/sec)
MXC.TAC.M.03-1001X-01#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

如果得到下一个输出，则文件传输失败：

```
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#
```

采取以下操作：

- 验证防火墙是否阻止了端口443、80和22。
- 验证网络设备阻止端口443或HTTPS协议中是否存在访问列表。
- 当传输文件时，向网络设备捕获数据包。



注意：完成测试HTTPS文件传输后，使用命令删除cisco-bridge.png文件 delete flash:cisco-bridge.png

---

网络设备中的HTTPS客户端源接口

验证您的网络设备中客户端源接口是否配置正确。

您可以运行 show run | in http client source-interface 命令以验证配置：

```
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#
```

如果设备的源接口不正确或缺少源接口，HTTPS传输文件测试将失败。

请看示例：

实验室设备的“Inventory Cisco DNA Center（库存思科DNA中心）”中包含IP地址10.88.174.43：

资产屏幕截图：

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文件传输测试失败：

```
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#
```

验证源接口：

<#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
```

检验接口：

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#

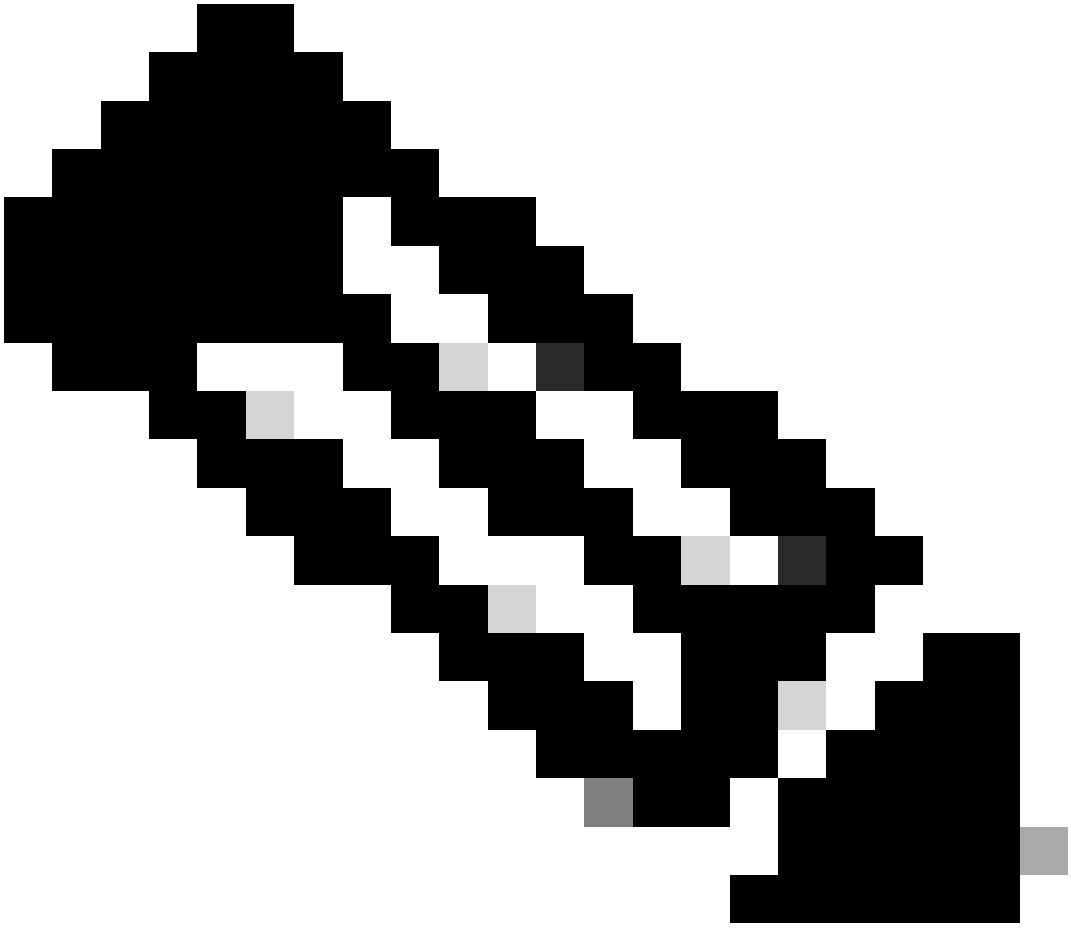
根据清单屏幕截图，思科DNA中心使用接口GigabitEthernet0而不是GigabiEthernet0/0/0发现了设备

您需要使用正确的源接口进行修改才能解决问题。

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：完成测试HTTPS文件传输后，使用命令删除cisco-bridge.png文件 delete flash:cisco-bridge.png

---

日期同步

使用命令检验网络设备日期和时钟是否正确 show clock

请考虑实验室设备中DNAC-CA证书缺失的实验场景。已推送遥测更新；但是，DNAC-CA证书安装失败，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

您可以看到，证书有效；但是，错误消息表明证书尚未生效或已过期。

验证网络设备时间：

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

日期和时间错误。要解决此问题，可以在特权模式下配置ntp服务器或使用命令clock set 手动配置时钟。

手动时钟配置示例：

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

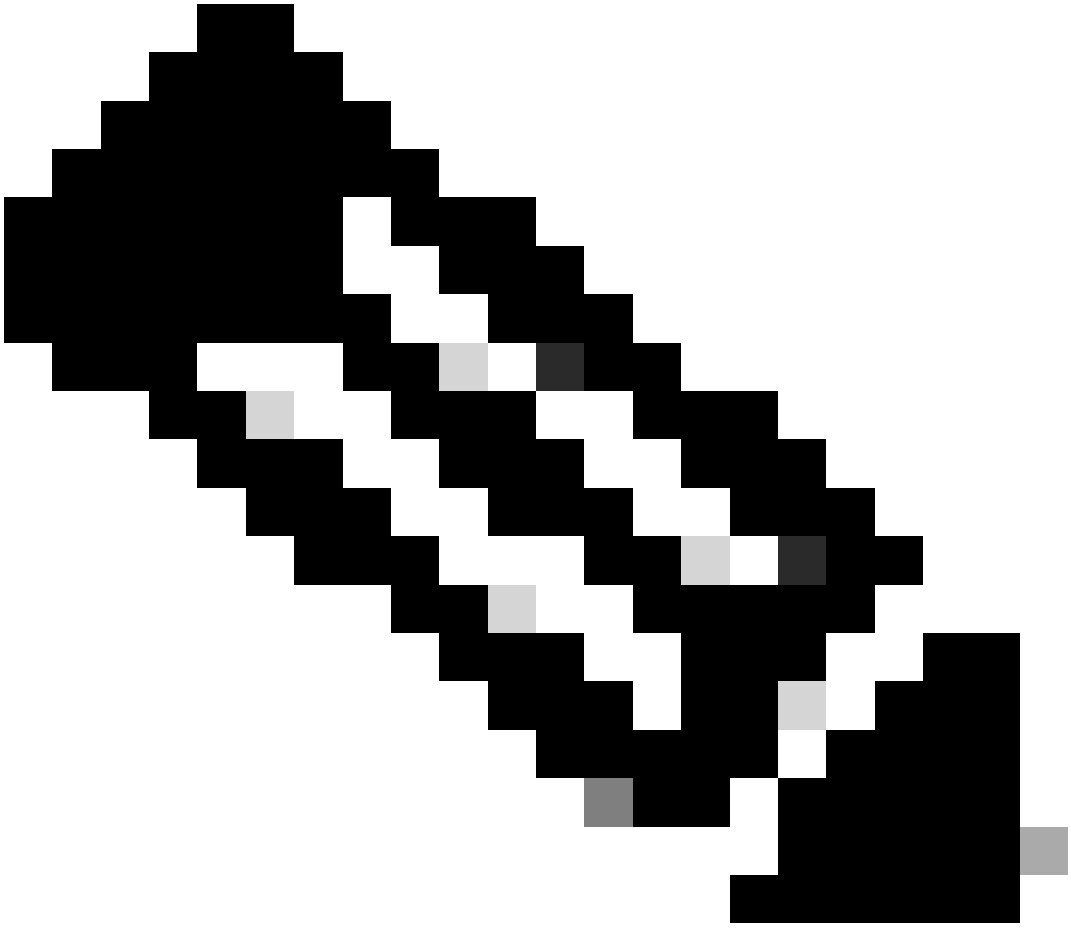
NTP配置示例：

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

调试

您可以运行调试来解决HTTPS问题：

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



注意：完成网络设备的故障排除后，请使用命令停止调试 undebug all

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。