Resolución de problemas de error HTTPS en el centro DNA para SWIM

Contenido

Introducción

Este documento describe un procedimiento para resolver problemas con el protocolo HTTPS en el proceso SWIM para Cisco DNA Center en plataformas Cisco IOS® XE.

Prerequisites

Requirements

Debe tener acceso a Cisco DNA Center a través de la GUI con privilegio ADMIN ROLE y la CLI del switch.

Componentes Utilizados

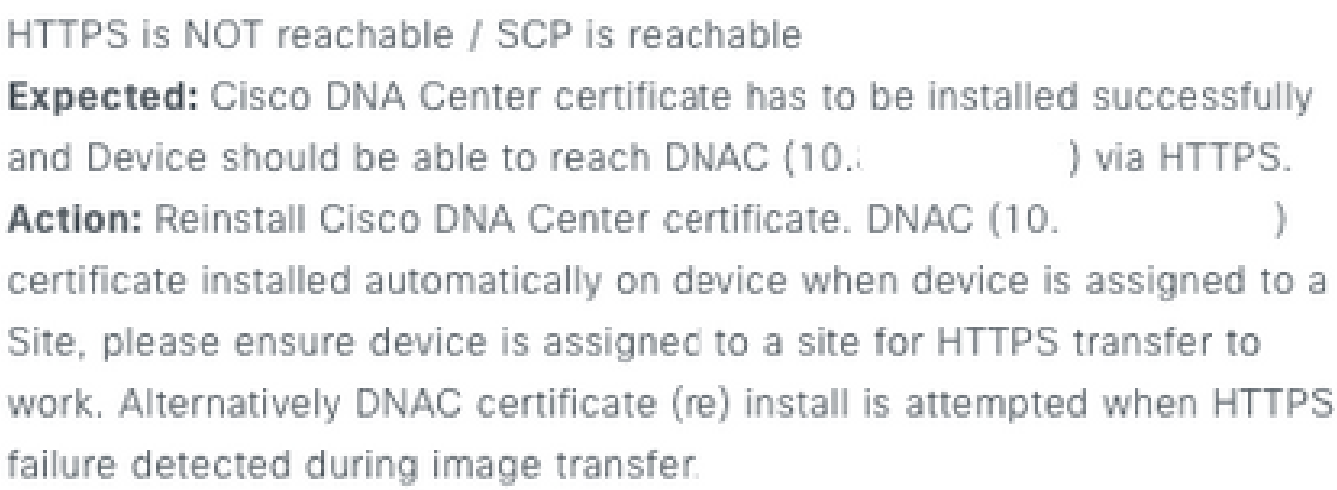
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

Hay un error común que Cisco DNA Center / Software Image Management (SWIM) muestra

después de la comprobación de idoneidad para la actualización de la imagen:

"NO se puede alcanzar HTTPS/SCP"



Este error describe que el protocolo HTTPS no es accesible; sin embargo, Cisco DNA Center va a utilizar el protocolo SCP para transferir la imagen de Cisco IOS® XE al dispositivo de red.

Una desventaja del uso de SCP es el tiempo que se tarda en distribuir la imagen. HTTPS es más rápido que SCP.

Verificación

Estado del dispositivo de red en el inventario de Cisco DNA Center

Navegue hasta Provisión > Inventario > Cambiar foco a Inventario

Verifique la disponibilidad y la capacidad de administración para que el dispositivo de red se actualice. El estado del dispositivo debe ser Reachable y Managed.

Si el dispositivo de red tiene cualquier otro estado en Disponibilidad y capacidad de gestión, corrija el problema antes de continuar con los siguientes pasos.

Certificado DNAC-CA instalado en el dispositivo de red

Vaya al dispositivo de red y ejecute el comando:

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

Debe ver el punto de confianza DNAC-CA y la cadena DNAC-CA. Si no puede ver el punto de confianza, la cadena o ambos de DNAC-CA, debe Actualizar la configuración de telemetría para insertar el certificado de DNAC-CA.

Si la capacidad de control del dispositivo está deshabilitada, instale el certificado DNAC-CA manualmente con los siguientes pasos:

- En un navegador web, escriba https://<dnac_ipaddress>/ca/pem y descargue el archivo .pem
- Guarde el archivo .pem en el equipo local
- Abrir un archivo .pem con una aplicación de editor de texto
- CLI de dispositivo de red abierto
- Verifique cualquier certificado de DNA-CA antiguo con el comando show run | in crypto pki trustpoint DNAC-CA

    - Si hay un certificado DNA-CA antiguo, elimine el certificado DNAC-CA con el comando no crypto pki trustpoint DNAC-CA en el modo de configuración

    - Ejecute los comandos en el modo de configuración para instalar el certificado DNAC-CA:

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

    - Pegar el archivo de texto .pem

    - Introduzca yes cuando se le solicite

    - Guarde la configuración

Resolución de problemas

Comunicación del dispositivo de red al centro DNA de Cisco en el dispositivo de red a través del puerto 443

Ejecute la prueba de transferencia de archivos HTTPS en el dispositivo de red

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

Esta prueba transfiere un archivo PNG desde Cisco DNA Center al switch.

Esta salida describe que la transferencia de archivos se ha realizado correctamente

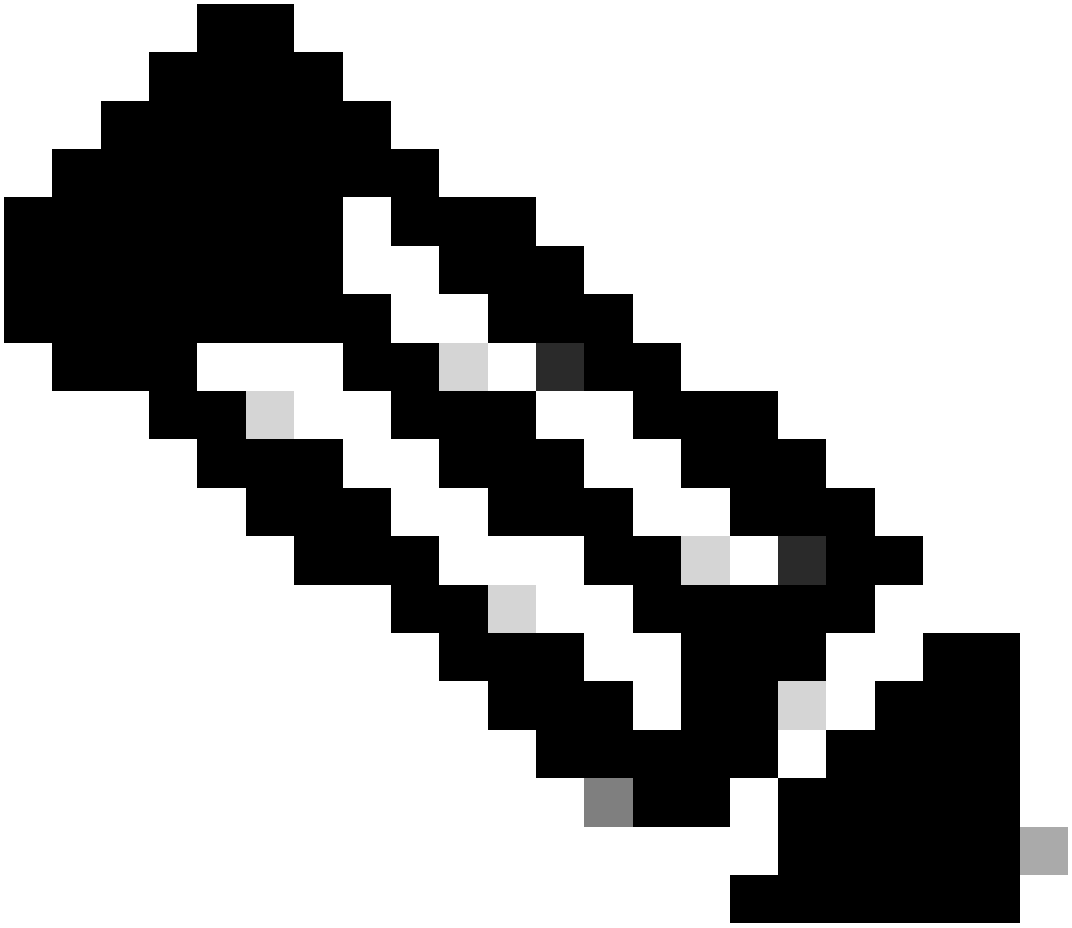
```
MXC.TAC.M.03-1001X-01#copy https://10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
Loading https://10.x.x.x/core/img/cisco-bridge.png
4058 bytes copied in 0.119 secs (34101 bytes/sec)
MXC.TAC.M.03-1001X-01#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

Si obtiene el siguiente resultado, la transferencia de archivos falló:

```
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#
```

Lleve a cabo las siguientes acciones:

- Compruebe si el firewall está bloqueando los puertos 443, 80 y 22.
- Verifique si existe una lista de acceso en el puerto de bloqueo del dispositivo de red 443 o en el protocolo HTTPS.
- Realice una captura de paquetes en el dispositivo de red mientras se realiza la transferencia de archivos.



Nota: Después de terminar de probar la transferencia de archivos HTTPS, elimine el archivo cisco-bridge.png con el comando delete flash:cisco-bridge.png

---

Interfaz de origen del cliente HTTPS en el dispositivo de red

Verifique que la interfaz de origen del cliente del dispositivo de red esté configurada correctamente.

Puede ejecutar el comando para validar show run | in http client source-interface la configuración:

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#

La prueba del archivo de transferencia HTTPS fallará si el dispositivo tiene una interfaz de origen incorrecta o falta la interfaz de origen.

Eche un vistazo al ejemplo:

El dispositivo de laboratorio tiene la dirección IP 10.88.174.43 en el Centro de ADN de Cisco del inventario:

Captura de pantalla del inventario:

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

Falló la prueba de transferencia de archivos HTTPS:

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#

Verificar interfaz de origen:

<#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
```

Verificar 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#

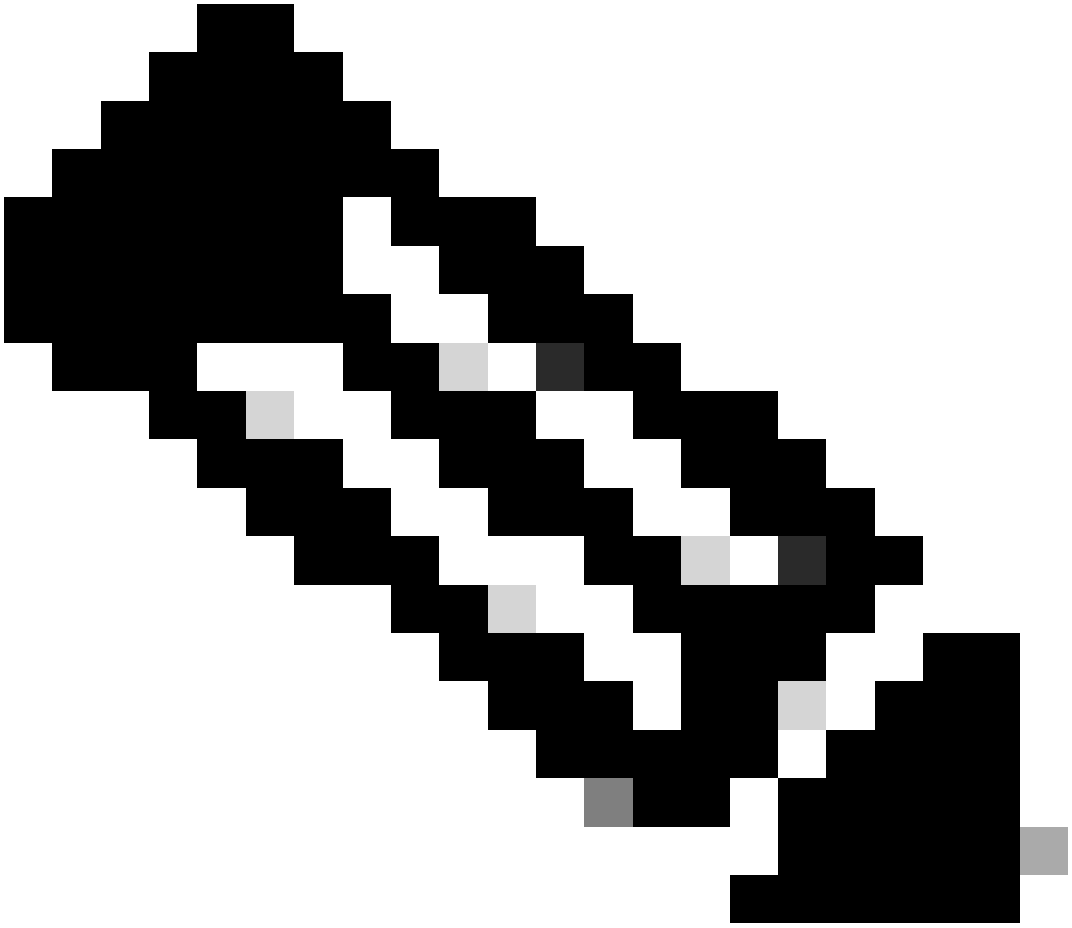
Según la captura de pantalla del inventario, Cisco DNA Center descubrió el dispositivo usando la interfaz GigabitEthernet0 en lugar de GigabitEthernet0/0/0

Debe modificar con la interfaz de origen correcta para solucionar el problema.

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#



Nota: Después de terminar de probar la transferencia de archivos HTTPS, elimine el archivo cisco-bridge.png con el comando delete flash:cisco-bridge.png

---

Sincronización de fecha

Verifique que el dispositivo de red tenga fecha y reloj correctos con el comando show clock

Eche un vistazo a la situación de laboratorio en la que faltaba el certificado DNAC-CA en el dispositivo LAB. Se insertó la actualización de telemetría; sin embargo, la instalación del certificado DNAC-CA falló debido a:

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

Como puede ver, el certificado es válido; sin embargo, el error indica que el certificado aún no es válido o que ha caducado.

Verifique la hora del dispositivo de red:

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

Se ha producido un error con la fecha y la hora. Para solucionar este problema, puede configurar un servidor ntp o configurar manualmente el reloj con el comando clock set en el modo de privilegio.

Ejemplo de configuración manual del reloj:

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

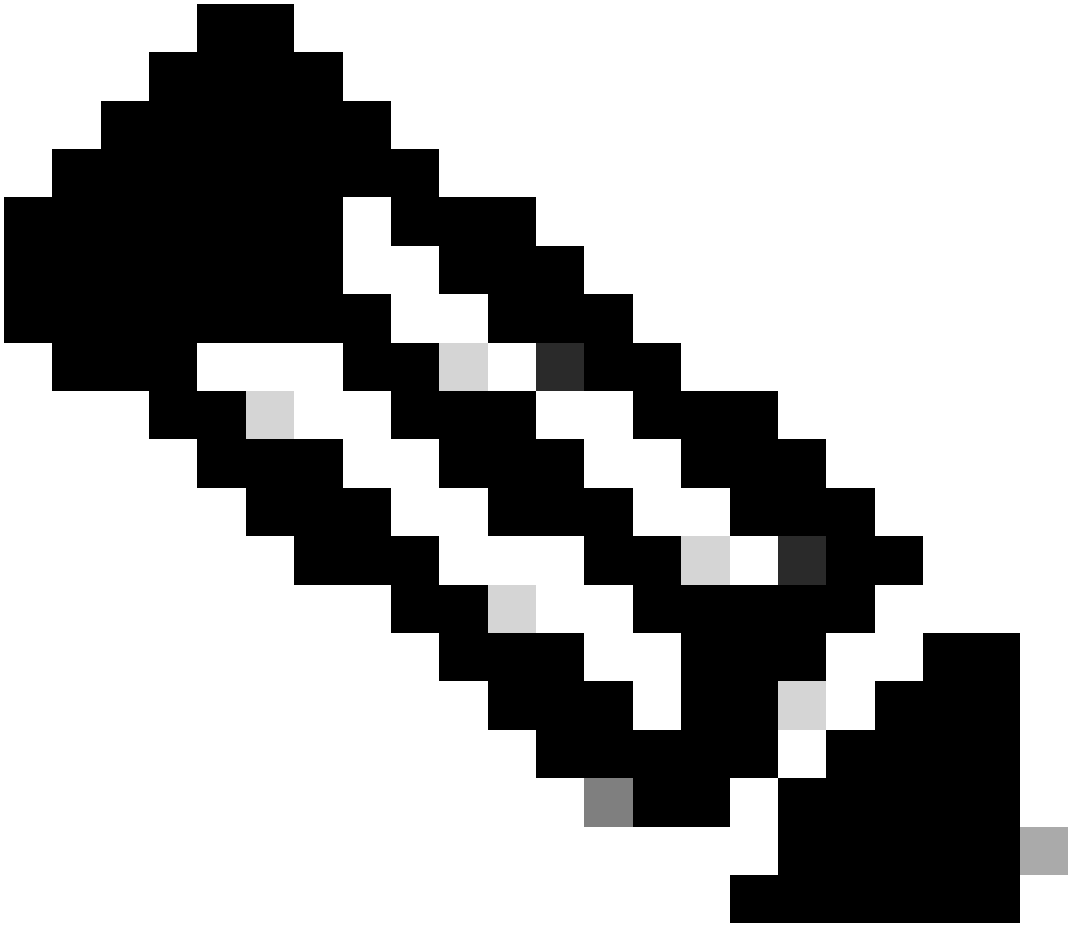
Ejemplo de configuración de NTP:

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

Depuraciones

Puede ejecutar depuraciones para solucionar problemas de HTTPS:

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



Nota: Después de terminar de resolver problemas del dispositivo de red, detenga las depuraciones con el comando undebug all

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).