Solucionar erros HTTPS no Cisco Catalyst Center para SWIM

Contents

Introdução

Este documento descreve um procedimento para solucionar problemas com o protocolo HTTPS no processo SWIM para o Cisco Catalyst Center nas plataformas Cisco IOS® XE.

Pré-requisitos

Requisitos

Você deve ter acesso ao Cisco Catalyst Center através da GUI com o privilégio ADMIN ROLE e a CLI do switch.

O Cisco Catalyst Center deve estar sendo executado em um dispositivo físico.

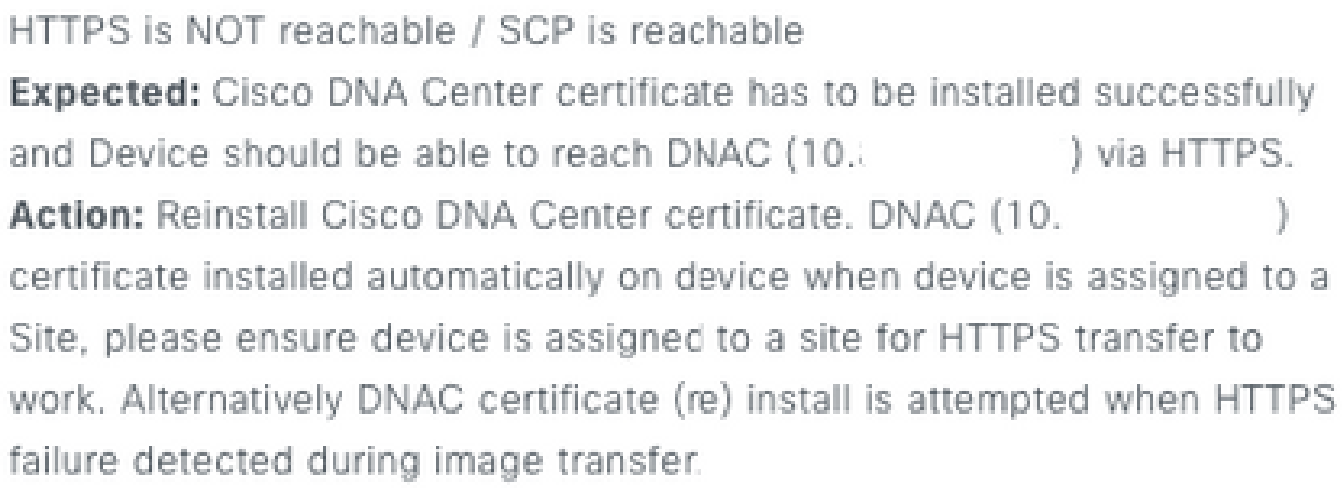
Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

Há um erro comum que o Cisco Catalyst Center / Software Image Management (SWIM) exibe após a Verificação de Preparação para Atualização de Imagem:

"HTTPS NÃO está acessível / SCP está acessível"



Esse erro descreve que o protocolo HTTPS não está acessível; no entanto, o Cisco Catalyst Center usará o protocolo SCP para transferir a imagem do Cisco IOS® XE para o dispositivo de rede.

Uma desvantagem do uso da SCP é o tempo necessário para distribuir a imagem. O HTTPS é mais rápido que o SCP.

Verificação

Status do dispositivo de rede no inventário do Cisco Catalyst Center

Navegue até Provisionar > Inventário > Alterar Foco para Inventário

Verifique a alcançabilidade e gerenciabilidade do dispositivo de rede a ser atualizado. O status do dispositivo deve ser Acessível e Gerenciado.

Se o dispositivo de rede tiver qualquer outro status em Acessibilidade e Capacidade de gerenciamento, corrija o problema antes de passar para as próximas etapas.

Certificado DNAC-CA instalado no Dispositivo de Rede

Vá até o dispositivo de rede e execute o comando:

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

Você deve ver o ponto de confiança DNAC-CA e a cadeia DNAC-CA. Se você não puder ver o ponto de confiança DNAC-CA, a cadeia ou ambos, será necessário Atualizar configurações de

telemetria para enviar o certificado DNAC-CA.

Se a capacidade de controle do dispositivo estiver desabilitada, instale manualmente o certificado DNAC-CA com as próximas etapas:

- Em um navegador da Web, digite https://<dnac_ipaddress>/ca/peme faça o download do arquivo .pem
- Salve o arquivo .pem no computador local
- Abrir arquivo .pem com um aplicativo de editor de texto
- CLI do dispositivo de rede aberta
- Verifique qualquer certificado DNA-CA antigo com o comando show run | in crypto pki trustpoint DNAC-CA

    - Se houver um certificado antigo do DNA-CA, remova o certificado do DNA-CA com o comando no crypto pki trustpoint DNAC-CA no modo de configuração

    - Execute os comandos no modo de configuração para instalar o 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
```

    - Colar o arquivo de texto .pem

    - Digite yes quando solicitado

    - Salve a configuração

Troubleshooting

Comunicação do Dispositivo de Rede com o Cisco Catalyst Center no Dispositivo de Rede através da porta 443

Executar o teste de transferência de arquivos HTTPS no dispositivo de rede

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

Este teste transfere um arquivo PNG do Cisco Catalyst Center para o switch.

Esta saída descreve que a transferência de arquivo foi bem-sucedida

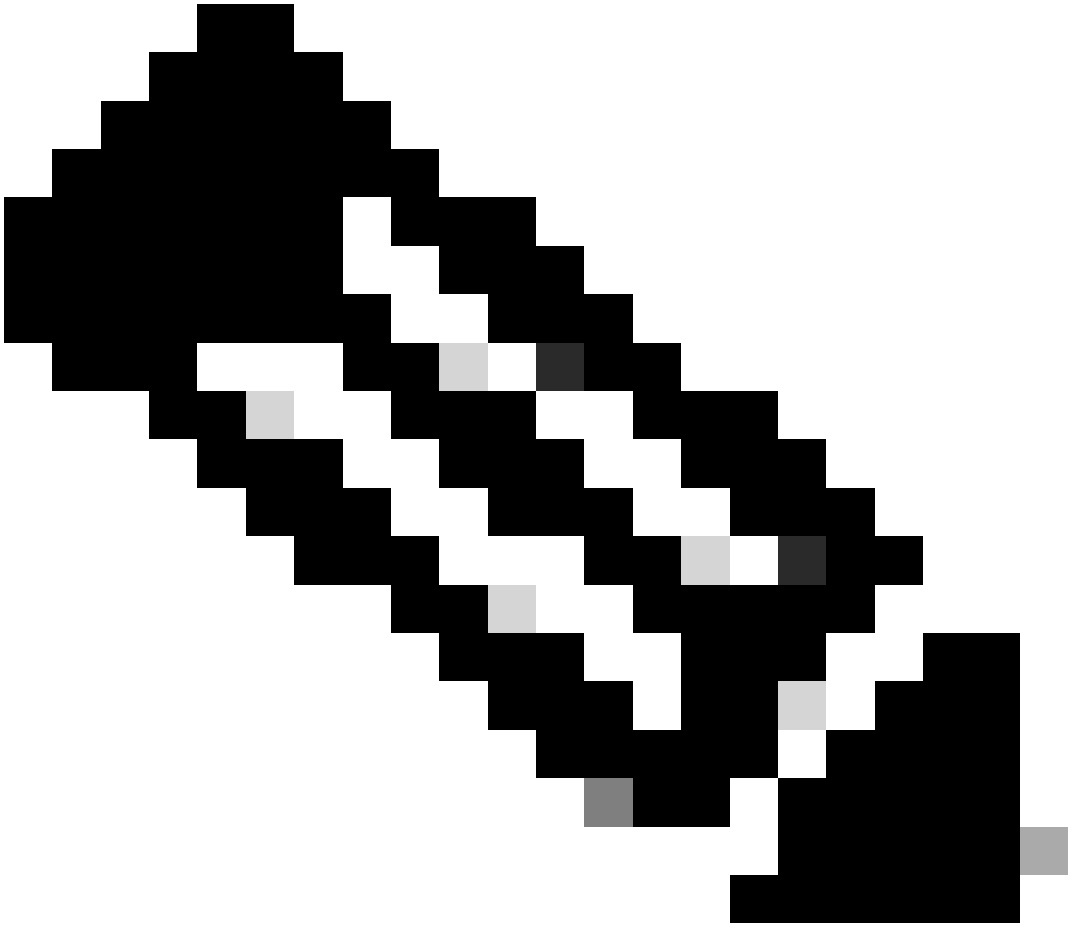
```
MXC.TAC.M.03-1001X-01#copy https://10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
Loading https://10.x.x.x/core/img/cisco-bridge.png
4058 bytes copied in 0.119 secs (34101 bytes/sec)
MXC.TAC.M.03-1001X-01#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

Se você obtiver a próxima saída, a transferência de arquivo falhará:

```
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#
```

Execute as próximas ações:

- Verifique se o firewall está bloqueando as portas 43, 80 e 22.
- Verifique se há uma lista de acesso no dispositivo de rede bloqueando a porta 443 ou o protocolo HTTPS.
- Faça uma captura de pacotes no dispositivo de rede enquanto ocorre a transferência de arquivos.



Observação: este procedimento não é válido com o Cisco Catalyst Virtual Appliance.

Depois de terminar de testar a transferência de arquivos HTTPS, remova o arquivo cisco-bridge.png com o comando delete flash:cisco-bridge.png

---

Interface-fonte do cliente HTTPS no dispositivo de rede

Verifique se a interface de origem do cliente do dispositivo de rede está configurada corretamente.

Você pode executar o comando show run | in http client source-interface para validar a configuração:

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#

O teste do arquivo de transferência HTTPS falhará se o dispositivo tiver uma interface de origem incorreta ou se a interface de origem estiver ausente.

Veja o exemplo:

O dispositivo do laboratório tem o endereço IP 10.88.174.43 no Inventário Cisco Catalyst Center:

Captura de tela do inventário:

Falha no teste de transferência de arquivo 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#

Verifique a interface de origem:

<#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#
```

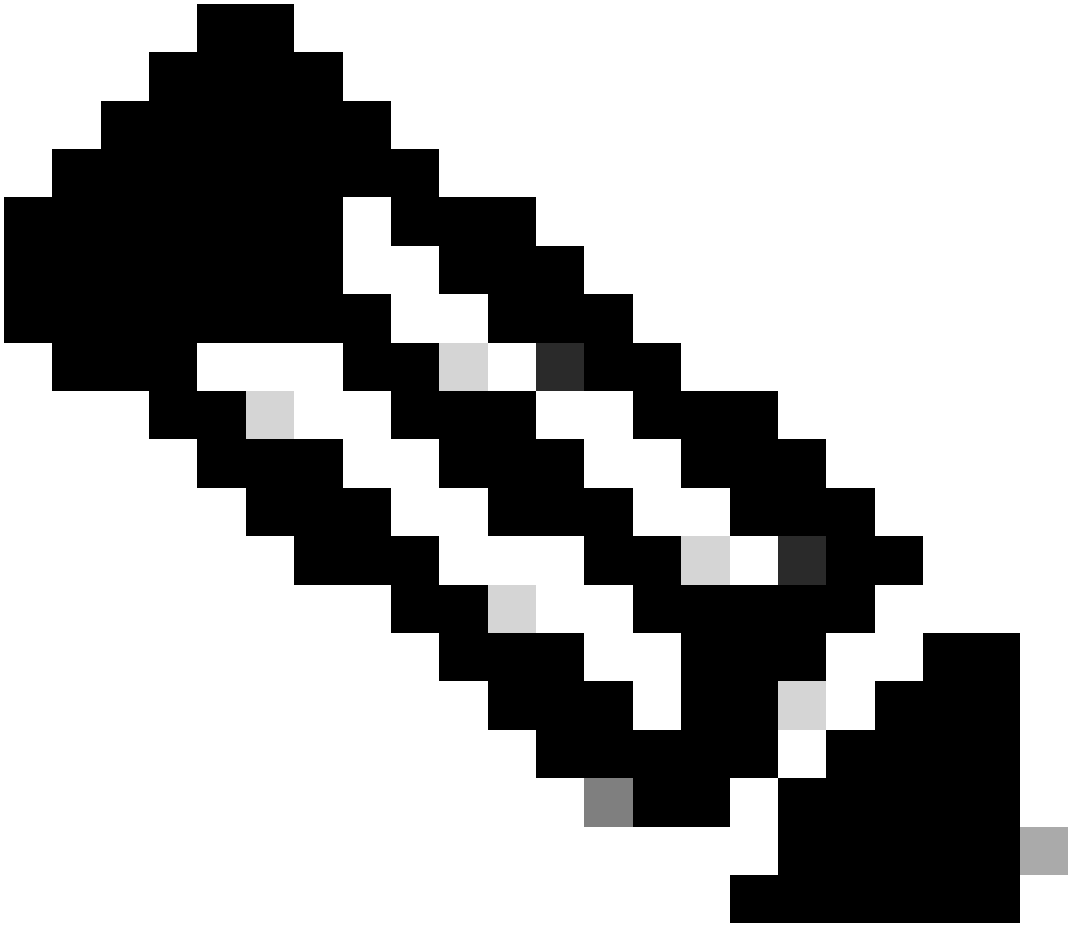
De acordo com a captura de tela do Inventário, o Cisco Catalyst Center descobriu o dispositivo usando a interface GigabitEthernet0 em vez de GigabitEthernet0/0/0

Você precisa modificar com a interface de origem correta para corrigir o 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#
```



Observação: depois que você terminar de testar a transferência de arquivos HTTPS, remova o arquivo cisco-bridge.png com o comando delete flash:cisco-bridge.png

---

Sincronização de data

Verifique se o dispositivo de rede tem a data e o relógio corretos com o comando show clock

Examine o cenário do laboratório em que o certificado DNAC-CA estava ausente no dispositivo do LAB. A atualização da telemetria foi enviada por push; no entanto, a instalação do certificado DNAC-CA falhou devido 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 você pode ver, o certificado é válido; no entanto, o erro diz que o certificado ainda não é válido ou expirou.

Verifique a hora do dispositivo de rede:

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

Erro na data e na hora. Para corrigir esse problema, você pode configurar um servidor ntp ou configurar manualmente o relógio com o comando clock set no modo privilegiado.

Exemplo de configuração manual do relógio:

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

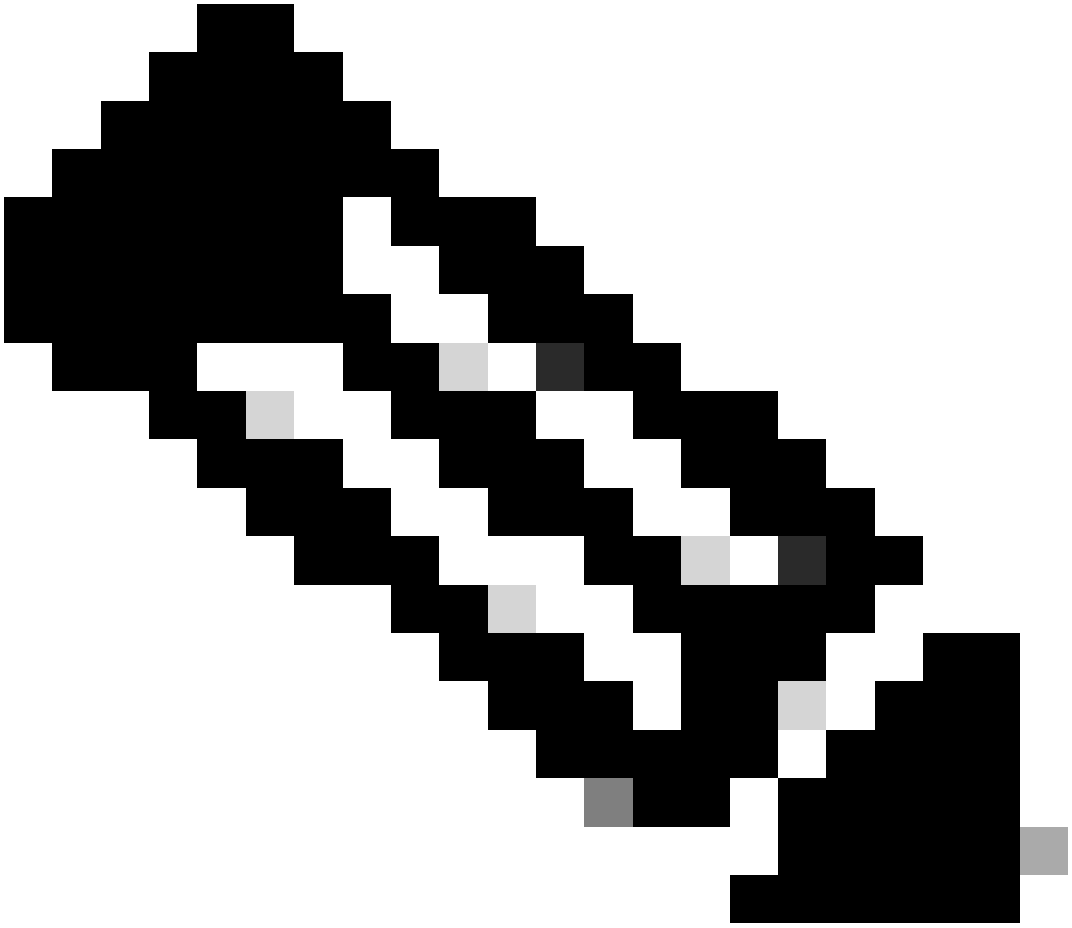
Exemplo de configuração de NTP:

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

Debugs

Você pode executar depurações para solucionar problemas de HTTPS:

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



Observação: depois de concluir a identificação e solução de problemas do dispositivo de rede, pare as depurações com o comando undebug all

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.