Dépannage d'une erreur HTTPS dans Cisco Catalyst Center pour SWIM

Table des matières

Introduction

Ce document décrit une procédure de dépannage des problèmes avec le protocole HTTPS dans le processus SWIM pour Cisco Catalyst Center dans les plates-formes Cisco IOS® XE.

Conditions préalables

Exigences

Vous devez avoir accès à Cisco Catalyst Center via l'interface utilisateur graphique avec le privilège RÔLE ADMIN et l'interface de ligne de commande du commutateur.

Cisco Catalyst Center doit être exécuté dans un appareil physique.

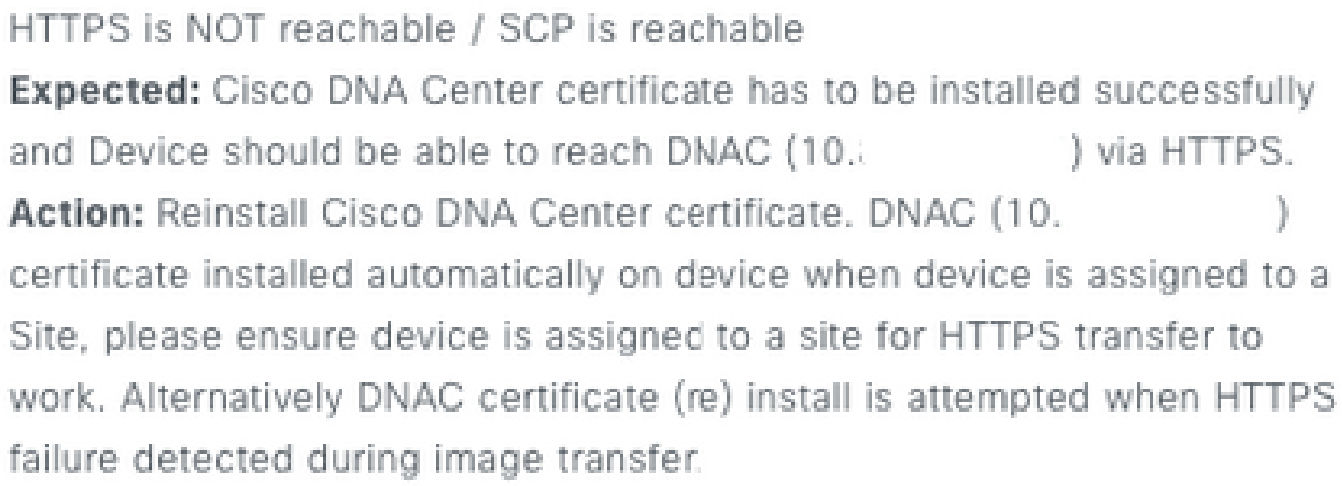
Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

Il y a une erreur courante que Cisco Catalyst Center / Software Image Management (SWIM) affiche après la vérification de l'état de préparation de la mise à jour d'image :

"HTTPS n'est PAS accessible / SCP est accessible"



Cette erreur indique que le protocole HTTPS n'est pas accessible. Toutefois, Cisco Catalyst Center va utiliser le protocole SCP pour transférer l'image Cisco IOS® XE vers le périphérique réseau.

L'un des inconvénients de la SCP est le temps nécessaire à la distribution de l'image. HTTPS est plus rapide que SCP.

Vérification

État des périphériques réseau dans Cisco Catalyst Center Inventory

Accédez à Provisionner > Stock > Modifier le focus en Stock

Vérifiez l'accessibilité et la facilité de gestion pour le périphérique réseau à mettre à niveau. L'état du périphérique doit être Accessible et Géré.

Si le périphérique réseau présente un autre état dans Accessibilité et facilité de gestion, résolvez le problème avant de passer aux étapes suivantes.

Certificat DNAC-CA installé dans le périphérique réseau

Accédez au périphérique réseau et exécutez la commande suivante :

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

Vous devez voir le point de confiance DNAC-CA et la chaîne DNAC-CA. Si vous ne pouvez pas voir le point de confiance DNAC-CA, la chaîne ou les deux, vous devez mettre à jour les

paramètres de télémétrie afin de transmettre le certificat DNAC-CA.

Si le contrôle du périphérique est désactivé, installez manuellement le certificat DNAC-CA en procédant comme suit :

- Dans un navigateur Web, tapez https://<dnac_ipaddress>/ca/pemand download the .pem file
- Enregistrez le fichier .pem sur votre ordinateur local
- Ouvrir un fichier .pem avec une application d'édition de texte
- Ouvrir la CLI du périphérique réseau
- Vérifiez tout ancien certificat DNA-CA avec la commande show run | in crypto pki trustpoint DNAC-CA

    - S'il existe un ancien certificat DNA-CA, supprimez DNAC-CA cert à l'aide de la commande no crypto pki trustpoint DNAC-CA en mode de configuration

    - Exécutez les commandes en mode de configuration afin d'installer DNAC-CA cert :

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

    - Coller le fichier texte .pem

    - Entrez yes lorsque vous y êtes invité

    - Enregistrez la configuration

Dépannage

Communication du périphérique réseau vers Cisco Catalyst Center dans le périphérique réseau via le port 443

Exécutez le test de transfert de fichiers HTTPS sur votre périphérique réseau

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

Ce test transfère un fichier PNG de Cisco Catalyst Center vers le commutateur.

Ce résultat décrit la réussite du transfert de fichiers

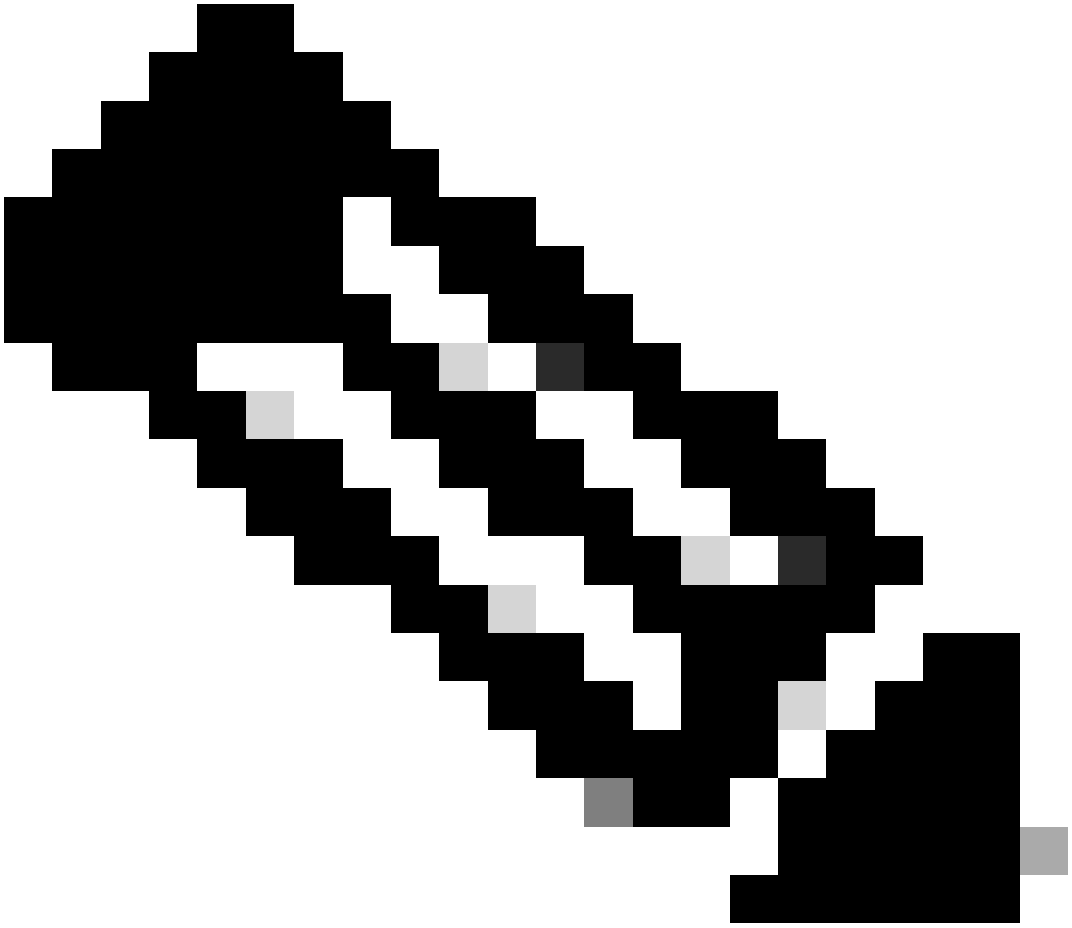
```
MXC.TAC.M.03-1001X-01#copy https://10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
Loading https://10.x.x.x/core/img/cisco-bridge.png
4058 bytes copied in 0.119 secs (34101 bytes/sec)
MXC.TAC.M.03-1001X-01#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

Si vous obtenez le résultat suivant, le transfert de fichier a échoué :

```
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#
```

Effectuez les actions suivantes :

- Vérifiez si le pare-feu bloque les ports 43, 80 et 22.
- Vérifiez s'il existe une liste d'accès dans le périphérique réseau bloquant le port 443 ou le protocole HTTPS.
- Effectuez une capture de paquets dans le périphérique réseau pendant le transfert de fichiers.



Remarque : ce marché n'est pas valide avec l'appliance virtuelle Cisco Catalyst.

Après avoir terminé de tester le transfert de fichiers HTTPS, supprimez le fichier cisco-bridge.png à l'aide de la commande delete flash:cisco-bridge.png

Interface source du client HTTPS dans le périphérique réseau

Vérifiez que l'interface source-client de votre périphérique réseau est correctement configurée.

Vous pouvez exécuter la commande show run | in http client source-interface afin de valider la configuration :

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#

Le test du fichier de transfert HTTPS va échouer si l'interface source du périphérique est incorrecte ou si l'interface source est manquante.

Examinez l'exemple suivant :

Le périphérique de TP a l'adresse IP 10.88.174.43 dans l'inventaire Cisco Catalyst Center :

Capture d'écran :

Échec du test de transfert de fichiers 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#

Vérifiez l'interface source :

<#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
```

Vérifiez les 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#

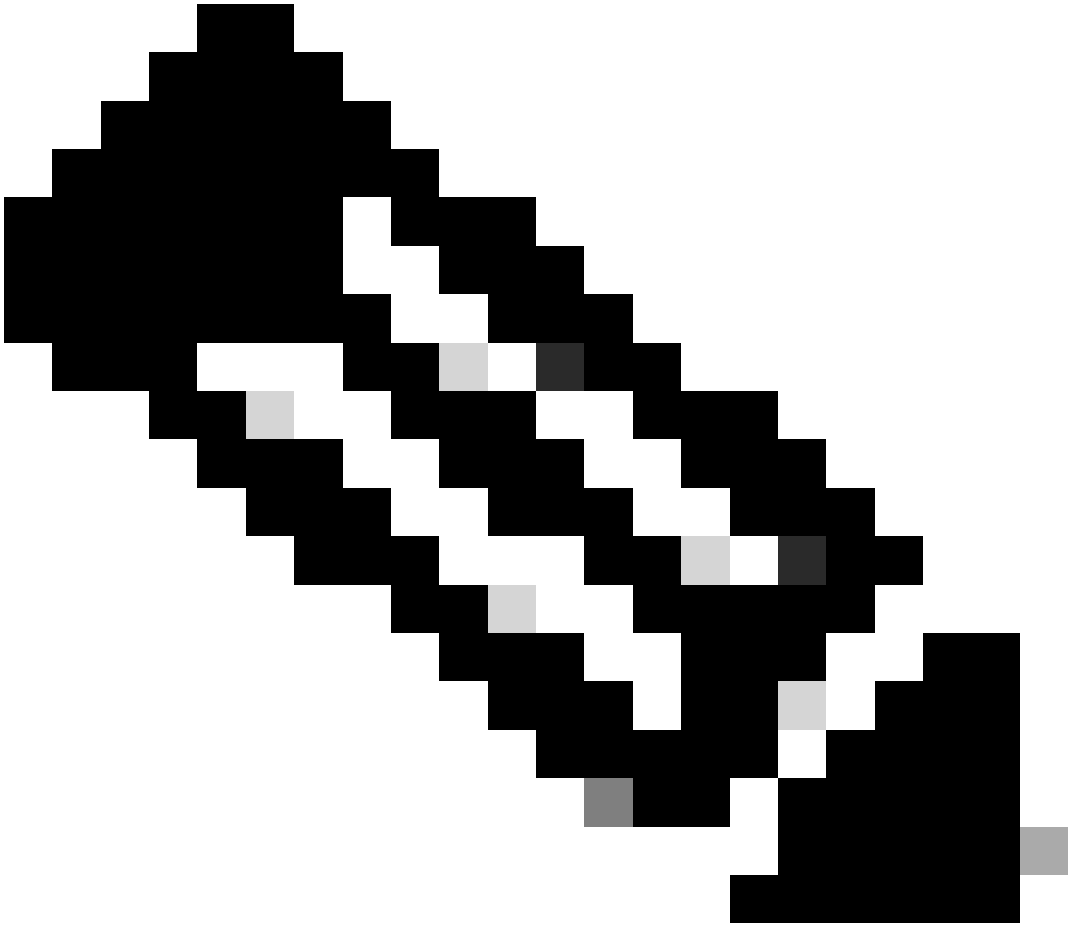
Selon la capture d'écran d'inventaire, Cisco Catalyst Center a découvert le périphérique en utilisant l'interface GigabitEthernet0 au lieu de GigabitEthernet0/0/0

Vous devez modifier avec l'interface source correcte afin de résoudre le problème.

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#



Remarque : une fois que vous avez terminé de tester le transfert de fichiers HTTPS, supprimez le fichier cisco-bridge.png à l'aide de la commande delete flash:cisco-bridge.png

---

Synchronisation de date

Vérifiez que la date et l'horloge du périphérique réseau sont correctes avec la commande show clock

Examinez le scénario des travaux pratiques dans lequel le certificat DNAC-CA était absent du périphérique des travaux pratiques. La mise à jour de télémétrie a été diffusée ; cependant, l'installation du certificat DNAC-CA a échoué en raison de :

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

Comme vous pouvez le voir, le certificat est valide ; cependant, l'erreur indique que le certificat n'est pas encore valide ou a expiré.

Vérifiez l'heure du périphérique réseau :

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

Une erreur s'est produite avec la date et l'heure. Afin de résoudre ce problème, vous pouvez configurer un serveur ntp ou configurer manuellement l'horloge avec la commande clock set en mode privilégié.

Exemple de configuration manuelle de l'horloge :

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

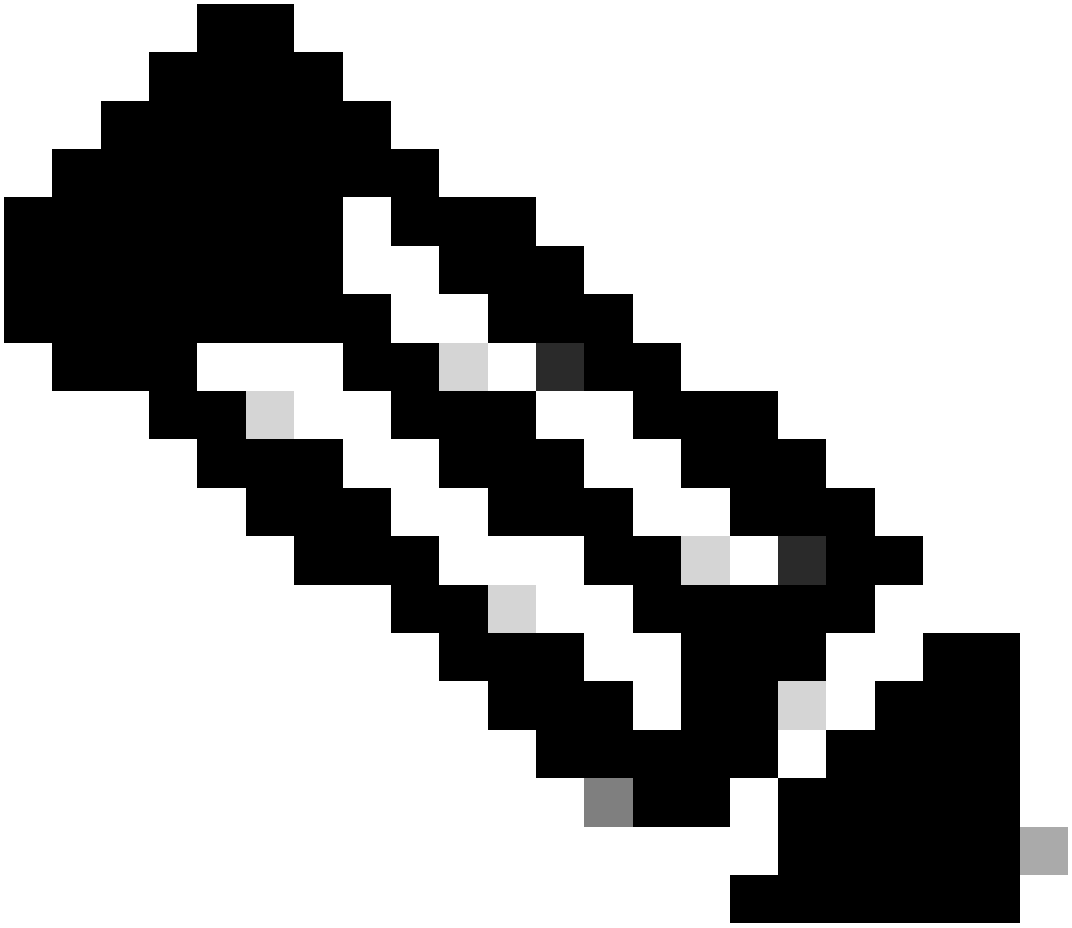
Exemple de configuration NTP :

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

Déboguages

Vous pouvez exécuter des débogages pour résoudre un problème HTTPS :

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



Remarque : une fois le dépannage du périphérique réseau terminé, arrêtez les débogages à l'aide de la commande undebug all

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.