Risoluzione dei problemi relativi all'errore HTTPS in Cisco Catalyst Center per SWIM

Sommario

Introduzione

Questo documento descrive una procedura per risolvere i problemi con il protocollo HTTPS nel processo SWIM per Cisco Catalyst Center nelle piattaforme Cisco IOS® XE.

Prerequisiti

Requisiti

È necessario disporre dell'accesso a Cisco Catalyst Center tramite la GUI con privilegio ADMIN ROLE e switch CLI.

Cisco Catalyst Center deve essere in esecuzione in un'appliance fisica.

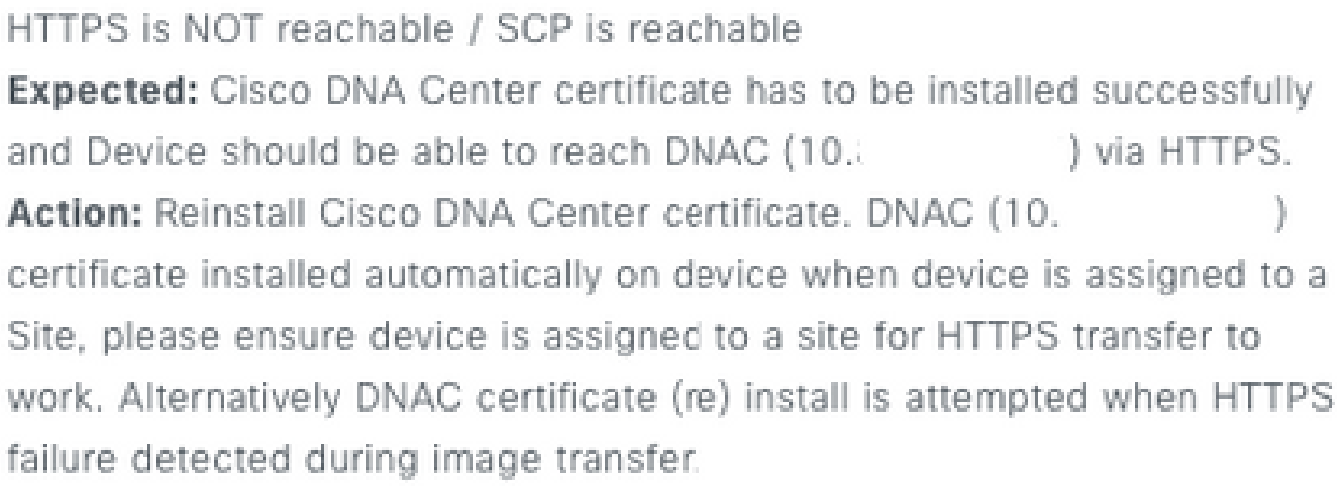
Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

È presente un errore comune che Cisco Catalyst Center/Software Image Management (SWIM) visualizza dopo il controllo della preparazione dell'aggiornamento dell'immagine:

"HTTPS NON è raggiungibile / SCP è raggiungibile"



In questo errore viene descritto che il protocollo HTTPS non è raggiungibile. Tuttavia, Cisco Catalyst Center utilizzerà il protocollo SCP per trasferire l'immagine Cisco IOS® XE al dispositivo di rete.

Uno svantaggio dell'utilizzo di SCP è la quantità di tempo necessaria per distribuire l'immagine. HTTPS è più veloce di SCP.

Verifica

Stato del dispositivo di rete nell'inventario del Cisco Catalyst Center

Passare a Accantonamento > Magazzino > Cambia stato attivo in Magazzino

Verificare Raggiungibilità e gestibilità per il dispositivo di rete da aggiornare. Lo stato del dispositivo deve essere Raggiungibile e Gestito.

Se il dispositivo di rete ha qualsiasi altro stato in Raggiungibilità e gestibilità, risolvere il problema prima di passare alla procedura successiva.

Certificato DNAC-CA installato nel dispositivo di rete

Andare al dispositivo di rete ed eseguire il comando:

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

È necessario visualizzare il trust point DNAC-CA e la catena DNAC-CA. Se non è possibile visualizzare il trust point, la catena o entrambi, è necessario aggiornare le impostazioni di

telemetria per eseguire il push del certificato DNAC-CA.

Se la funzionalità di controllo del dispositivo è disattivata, installare manualmente il certificato DNAC-CA seguendo la procedura seguente:

- In un browser Web digitare https://<indirizzo_ip_dnac>/ca/pemand per scaricare il file .pem
- Salvare il file con estensione pem nel computer locale
- Aprire il file con estensione pem con un'applicazione di editor di testo
- Apri CLI dispositivo di rete
- Verificare qualsiasi certificato DNA-CA precedente con il comando show run | in crypto pki trustpoint DNAC-CA

    - Se è presente un certificato DNA-CA precedente, rimuovere il certificato DNAC-CA con il comando no crypto pki trustpoint DNAC-CA in modalità di configurazione

    - Per installare il certificato DNAC-CA, eseguire i comandi in modalità di configurazione:

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

    - Incollare il file di testo con estensione pem

    - Quando richiesto, immettere yes

    - Salvare la configurazione

Risoluzione dei problemi

Comunicazione tra dispositivo di rete e Cisco Catalyst Center nel dispositivo di rete tramite la porta 443

Eseguire il test di trasferimento file HTTPS nel dispositivo di rete

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

Questo test consente di trasferire un file PNG da Cisco Catalyst Center allo switch.

Questo output descrive il completamento del trasferimento di file

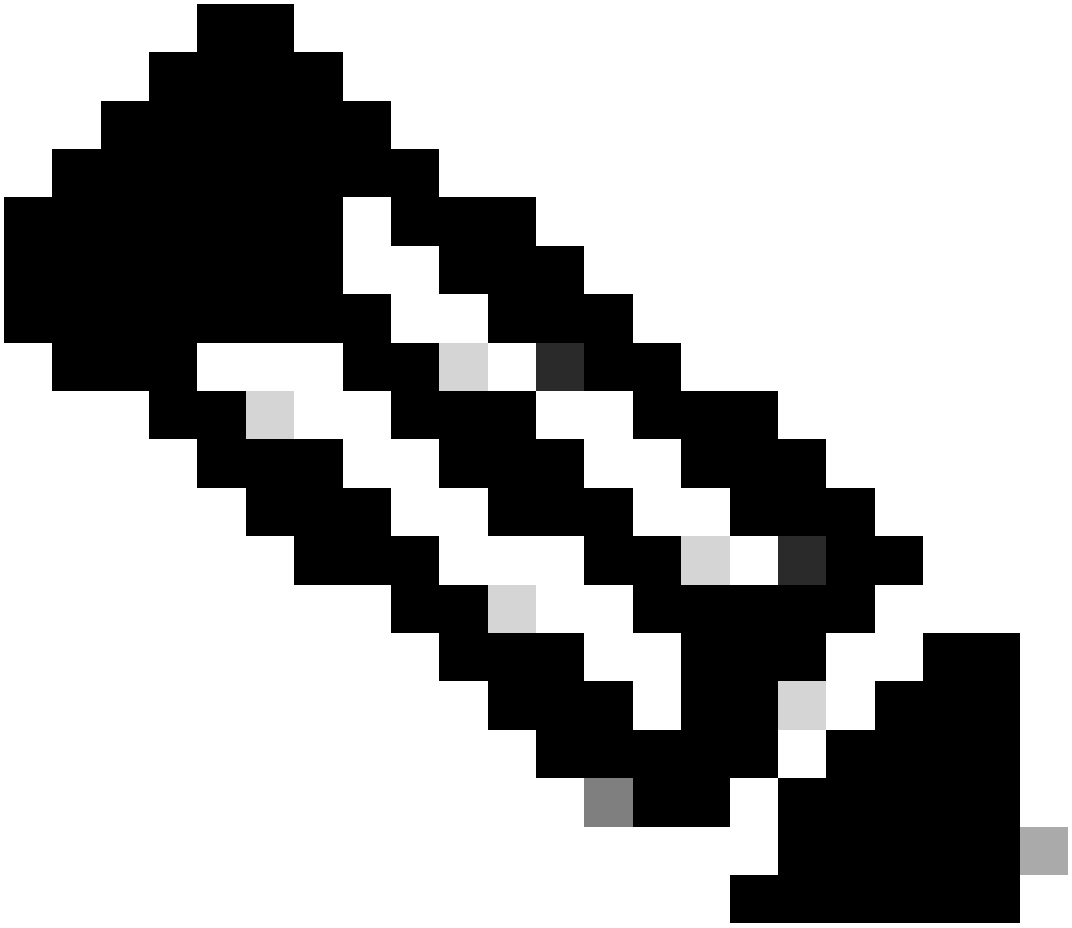
```
MXC.TAC.M.03-1001X-01#copy https://10.x.x.x/core/img/cisco-bridge.png flash:
Destination filename [cisco-bridge.png]?
Accessing https://10.x.x.x/core/img/cisco-bridge.png...
Loading https://10.x.x.x/core/img/cisco-bridge.png
4058 bytes copied in 0.119 secs (34101 bytes/sec)
MXC.TAC.M.03-1001X-01#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

Se si ottiene l'output successivo, il trasferimento del file non è riuscito:

```
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#
```

Eseguire le azioni successive:

- Verificare se il firewall blocca le porte 443, 80 e 22.
- Verificare se è presente un elenco degli accessi nel dispositivo di rete che blocca la porta 443 o il protocollo HTTPS.
- Acquisire un pacchetto nel dispositivo di rete durante il trasferimento dei file.



Nota: questa procedura non è valida con Cisco Catalyst Virtual Appliance.

Dopo aver terminato di verificare il trasferimento del file HTTPS, rimuovere il file cisco-bridge.png con il comando delete flash:cisco-bridge.png

---

Interfaccia di origine client HTTPS nel dispositivo di rete

Verificare che l'interfaccia dell'origine client del dispositivo di rete sia configurata correttamente.

È possibile eseguire il comando show run | in http client source-interface per convalidare la configurazione:

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#

Il test del file di trasferimento HTTPS avrà esito negativo se il dispositivo ha un'interfaccia di origine non corretta o se l'interfaccia di origine è mancante.

Osservate l'esempio:

Il dispositivo lab ha l'indirizzo ip 10.88.174.43 in Inventory Cisco Catalyst Center:

Schermata 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

Test di trasferimento file HTTPS non riuscito:

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#

Verificare l'interfaccia di origine:

<#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
```

Verifica interfacce:

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#
```

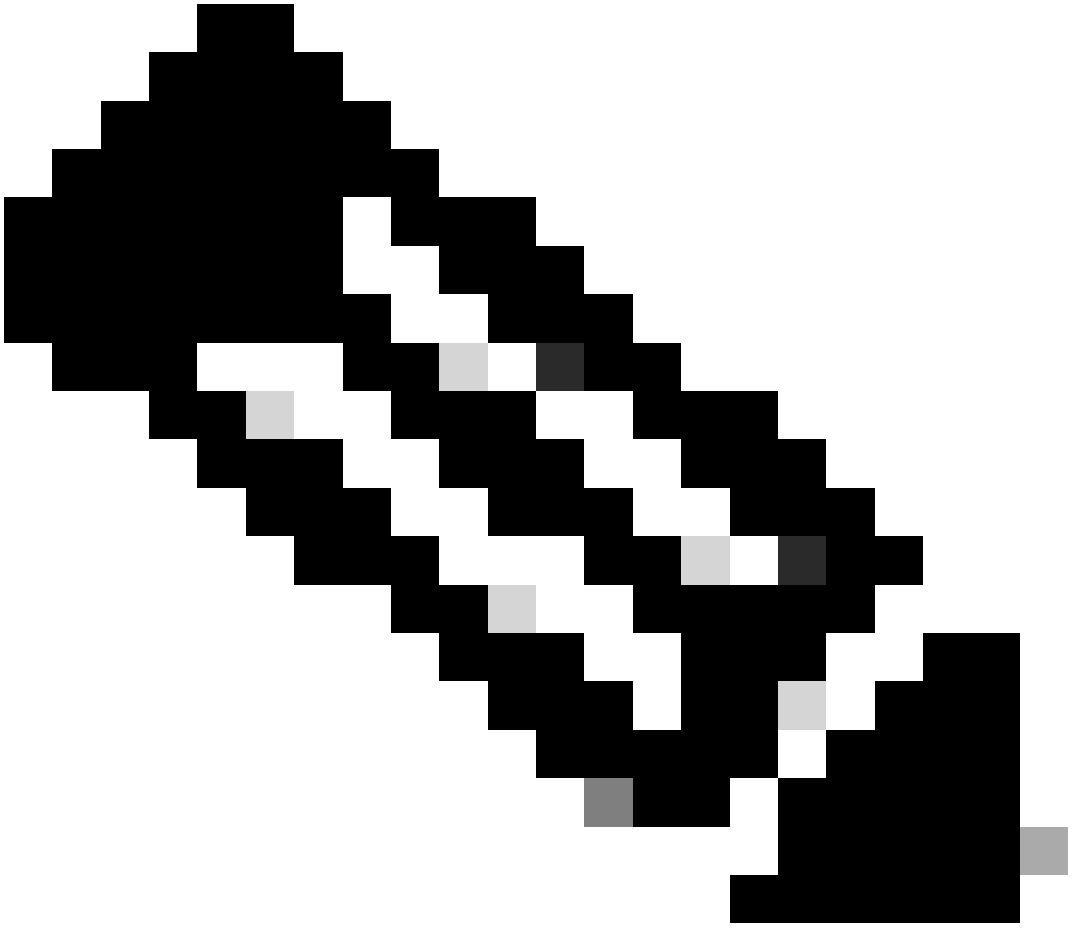
In base alla schermata di inventario, Cisco Catalyst Center ha rilevato il dispositivo utilizzando l'interfaccia Gigabit Ethernet0 anziché Gigabit Ethernet0/0/0

Per risolvere il problema, è necessario apportare delle modifiche utilizzando l'interfaccia di origine corretta.

```
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: dopo aver completato il test del trasferimento dei file HTTPS, rimuovere il file cisco-bridge.png con il comando delete flash:cisco-bridge.png

---

Sincronizzazione data

Verificare che la data e l'ora del dispositivo di rete siano corrette con il comando show clock

Esaminare lo scenario lab in cui il certificato DNAC-CA risulta mancante nel dispositivo LAB. È stato eseguito il push dell'aggiornamento di telemetria. L'installazione del certificato DNAC-CA non è riuscita a causa di:

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

Come si può vedere, il certificato è valido; tuttavia, l'errore ha indicato che il certificato non è ancora valido o è scaduto.

Verificare l'ora del dispositivo di rete:

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

Errore nella data e nell'ora. Per risolvere il problema, è possibile configurare un server ntp o configurare manualmente l'orologio con il comando clock set in modalità privilegiata.

Esempio di configurazione manuale dell'orologio:

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

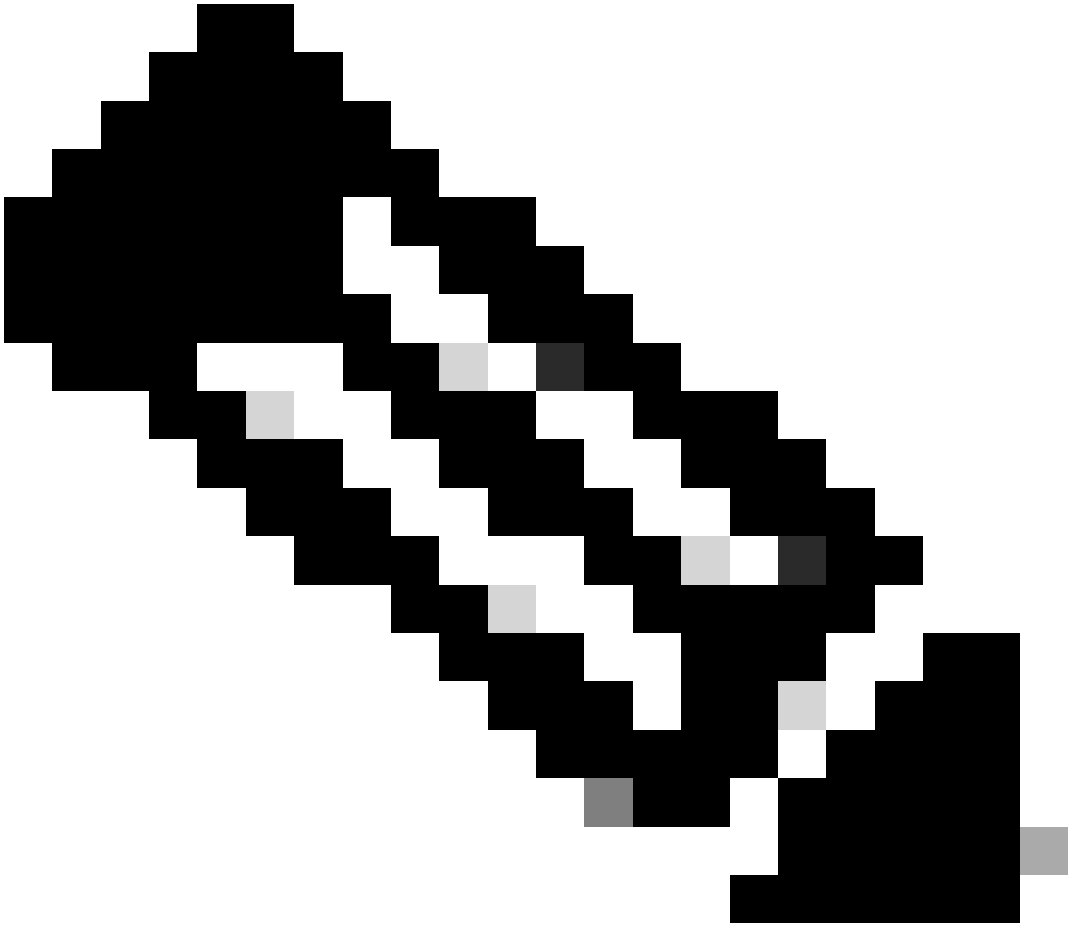
Esempio di configurazione NTP:

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

Debug

È possibile eseguire i debug per risolvere il problema HTTPS:

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



Nota: dopo aver completato la risoluzione dei problemi del dispositivo di rete, interrompere i debug con il comando undebug all

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).