Risoluzione dei problemi relativi all'assenza di dati di garanzia in WLC 9800 su Cisco Catalyst Center

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi quando Cisco Catalyst Center non visualizza dati Assurance per un Catalyst serie 9800 Wireless LAN Controller (WLC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Uso della maglev CLI di Catalyst Center
- Base Linux
- Conoscenza dei certificati sul Catalyst Center e sulla piattaforma Catalyst 9800

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Appliance Catalyst Center di prima o seconda generazione con software versione 1.x o 2.x con pacchetto Assurance
- Catalyst serie 9800 WLC

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.

Nota: sebbene questo documento sia stato inizialmente redatto per Catalyst Center 1.x, la maggior parte è valida per Catalyst Center 2.x.

Nota: Catalyst 9800 WLC deve essere già stato individuato da Catalyst Center e assegnato a un sito e deve eseguire una versione Cisco IOS® XE compatibile. Per ulteriori informazioni sull'interoperabilità, consultare la matrice di compatibilità di Catalyst Center.

Premesse

Al momento del processo di rilevamento, Catalyst Center passa la configurazione successiva al WLC.

Nota: questo esempio fa riferimento a Catalyst 9800-CL Cloud Wireless Controller. Quando si usa un accessorio Catalyst serie 9800 fisico, alcuni dettagli possono essere diversi; X.X.X.X è l'indirizzo IP virtuale (VIP) dell'interfaccia Enterprise di Catalyst Center e Y.Y.Y.Y è l'indirizzo IP di gestione del WLC.

<#root>

```
crypto pki trustpoint sdn-network-infra-iwan
 enrollment pkcs12
 revocation-check crl
 rsakeypair sdn-network-infra-iwan

crypto pki trustpoint DNAC-CA
 enrollment mode ra
 enrollment terminal
 usage ssl-client
 revocation-check crl none
 source interface GigabitEthernet1

crypto pki certificate chain sdn-network-infra-iwan
 certificate 14CFB79EFB61506E
  3082037D 30820265 A0030201 02020814 CFB79EFB 61506E30 0D06092A 864886F7
  <snip>
        quit

 certificate ca 7C773F9320DC6166
  30820323 3082020B A0030201 0202087C 773F9320 DC616630 0D06092A 864886F7
  <snip>
        quit

crypto pki certificate chain DNAC-CA
 certificate ca 113070AFD2D12EA443A8858FF1272F2A
  30820396 3082027E A0030201 02021011 3070AFD2 D12EA443 A8858FF1 272F2A30
  <snip>
        quit
```

```
telemetry ietf subscription 1011
 encoding encode-tdl
 filter tdl-uri /services;serviceName=ewlc/wlan_config
 source-address
```

Y.Y.Y.Y

```
 stream native
 update-policy on-change
 receiver ip address
```

X.X.X.X

```
 25103 protocol tls-native profile sdn-network-infra-iwan

telemetry ietf subscription 1012
<snip - many different "telemetry ietf subscription" sections - which ones depends on
Cisco IOS version and Catalyst Center version>

network-assurance enable
network-assurance icap server port 32626
network-assurance url https://
```

X.X.X.X

```
network-assurance na-certificate PROTOCOL_HTTP
```

X.X.X.X

```
 /ca/ pem
```

Risoluzione dei problemi relativi all'assenza di dati di garanzia dal WLC su Catalyst Center

Passaggio 1. Verificare che il WLC sia raggiungibile e gestito nell'inventario del Catalyst Center.

Se lo stato del WLC non è Gestito, è necessario risolvere il problema di raggiungibilità o provisioning prima di continuare.

Suggerimento: controllare i registri di inventory-manager, spf-device-manager e spf-service-manager per identificare l'errore.

Passaggio 2. Verificare che Catalyst Center trasferisca tutte le configurazioni necessarie al WLC.

Verificare che la configurazione indicata nella sezione Background Information sia stata trasferita sul WLC con questi comandi:

```
show run | section crypto pki trustpoint DNAC-CA
show run | section crypto pki trustpoint sdn-network-infra-iwan
show run | section network-assurance
show run | section telemetry
```

Problemi noti:

- Cisco bug ID CSCvs62939 - Cisco DNA Center non esegue il push della configurazione di telemetria sugli switch 9xxx dopo il rilevamento.
- ID bug Cisco CSCvt83104 - Errore di push della configurazione di WLC Assurance se l'archivio dati candidato Netconf è presente nel dispositivo.
- ID bug Cisco CSCvt97081 - Impossibile eseguire il provisioning dei certificati DNAC-CA WLC per il dispositivo rilevato dal nome DNS.

Registri da verificare:

- dna-wireless-service - per certificato DNAC-CA e configurazione di telemetria.
- network-design-service - per certificato sdn-network-infra-iwan.

Passaggio 3. Verificare che i certificati necessari vengano creati sul WLC.

Verificare che i certificati vengano creati correttamente sul WLC con questi comandi:

```
show crypto pki certificates DNAC-CA
show crypto pki certificates sdn-network-infra-iwan
```

Problemi noti e limitazioni:

- ID bug Cisco CSCvu03730 - Il WLC non è monitorato in Cisco DNA Center perché il certificato sdn-network-infra-iwan non è installato (la causa principale è che il certificato client pki-broker è scaduto).
- ID bug Cisco CSCvr44560 - ITA: aggiunge il supporto per i certificati CA che scadono dopo il 2099 per IOS-XE
- ID bug Cisco CSCwc99759 - ENH: aggiunta del supporto per la firma del certificato RSA a 8192 bit

Passaggio 4. Verificare lo stato della connessione telemetrica.

Verificare che la connessione di telemetria sia nello "Active" stato sul WLC con questo comando:

<#root>

```
wlc-01#
show telemetry internal connection

Telemetry connection

Address          Port   Transport   State          Profile
-----------------------------------------------------------------
X.X.X.X       25103  tls-native
Active
```

```
     sdn-network-infra-iwan
```

O da Cisco IOS XE versione 17.7 e successive:

```
<#root>

wlc-01#

show telemetry connection all


Telemetry connections

Index Peer Address               Port  VRF Source Address             State      State Description
----- ------------------------- ----- --- ------------------------- ---------- --------------------
 9825 X.X.X.X                    25103 0   Y.Y.Y.Y

Active

     Connection up
```

L'indirizzo IP X.X.X.X deve essere l'interfaccia Catalyst Center Enterprise. Se il Catalyst Center è configurato con VIP, deve essere il VIP dell'interfaccia Enterprise. Se l'indirizzo IP è corretto e lo stato è "Active", procedere al passaggio successivo.

Se lo stato è, "Connecting" la connessione HTTPS (Hypertext Transfer Protocol Secure) dal WLC al Catalyst Center non è stata stabilita correttamente. Ci possono essere molti motivi diversi per questo, i più comuni sono elencati di seguito.

4.1. L'indirizzo VIP del Catalyst Center non è raggiungibile dal WLC o è in "DOWN" stato.

- In un singolo nodo con VIP, il VIP diventa inattivo quando l'interfaccia del cluster diventa inattiva. Verificare che l'interfaccia del cluster sia connessa.
- Verificare che il WLC sia connesso all'indirizzo VIP organizzazione (ICMP/ping).
- Verificare che l'indirizzo VIP Catalyst Center Enterprise sia nello "UP" stato con questo comando: **ip a | grep en.**
- Verificare che l'indirizzo VIP dell'organizzazione di Catalyst Center sia configurato correttamente con questo comando: **etcdctl get /maglev/config/cluster/cluster_network.**

4.2. Il WLC è ad alta disponibilità (HA), Assurance non funziona dopo il failover.

Ciò può verificarsi se HA non è formato dal Catalyst Center. In tal caso: rimuovere il WLC da Inventory, interrompere l'HA, individuare entrambi i WLC e lasciare che Catalyst Center formi l'HA.

Nota: questo requisito può cambiare nelle versioni successive di Catalyst Center.

4.3. Catalyst Center non ha creato il trust point e il certificato DNAC-CA.

- Per risolvere il problema, controllare i passaggi 2 e 3.

4.4. Catalyst Center non ha creato il sdn-network-infra-iwan trust point e il certificato.

- Per risolvere il problema, controllare i passaggi 2 e 3.

4.5. Catalyst Center non ha eseguito il push della configurazione Assurance.

- Il comando **show network-assurance summary** mostra Network-Assurance come **Disabled**:

<#root>

```
DC9800-WLC#

show network-assurance summary

-------------------------------------------------
Network-Assurance                       :

Disabled

Server Url                              :
ICap Server Port Number            :
Sensor Backhaul SSID                    :
Authentication                          : Unknown
```

- Verificare che il WLC abbia la funzionalità di controllo dei dispositivi abilitata, in quanto è necessaria per il push della configurazione da parte di Catalyst Center. La funzione di controllo dei dispositivi può essere abilitata nel processo di rilevamento o quando il WLC si trova nell'inventario e viene gestito dal Catalyst Center. Passare alla **Inventory** pagina. Selezionare **Device** > **Actions** > **Inventory** > **Edit Device** > **Device Controllability** > **Enable**.

4.6. Catalyst Center non esegue il push della configurazione di sottoscrizione della telemetria.

- Verificare che il WLC disponga delle sottoscrizioni con il **show telemetry ietf subscription all** comando.
- In caso contrario, controllare i passaggi 2 e 3 per risolvere il problema.

4.7. L'handshake TLS tra il WLC e il Catalyst Center ha esito negativo perché il certificato del Catalyst Center non può essere convalidato dal WLC.

Ciò può essere dovuto a molti motivi, i più comuni sono elencati qui:

4.7.1 Il certificato Catalyst Center è scaduto o revocato oppure l'indirizzo IP del Catalyst Center non è incluso nel nome alternativo del soggetto (SAN).

- Verificare che il certificato corrisponda alle best practice specificate nella Guida alle best practice per la sicurezza di Catalyst Center.

4.7.2. Il controllo di revoca ha esito negativo perché non è possibile recuperare l'elenco di revoche di certificati (CRL).

- I motivi per cui il recupero della CRL non riesce possono essere diversi, ad esempio un errore DNS, un problema del firewall, un problema di connettività tra il WLC e il punto di

distribuzione della CRL (CDP) o uno dei seguenti problemi noti:
    - ID bug Cisco CSCvr41793 - PKI: per il recupero CRL non viene utilizzato HTTP Content-Length.
    - Cisco ID bug CSCvo03458 - Se l'elenco di revoche (CRL) non è raggiungibile, non viene eseguito il fallback dell'indicatore di revoche (CRL) PKI.
    - ID bug Cisco CSCue73820 - I debug PKI non sono chiari in caso di errore di analisi CRL.
- Per ovviare al problema, configurare **revocation-check none** il trust tra DNAC e CA.

4.7.3. Errore del certificato "Catena di certificati peer troppo lunga per essere verificata".

- Controllare l'output del **show platform software trace message mdt-pubd chassis active R** comando.
- Se viene visualizzato, **"Peer certificate chain is too long to be verified"** verificare quanto segue:

  Cisco ID bug CSCvw09580 - 9800 WLC non accetta la profondità delle catene di certificati Cisco DNA Center con 4 o più.

- Per risolvere questo problema, importare il certificato dell'autorità di certificazione intermedia che ha rilasciato il certificato del Catalyst Center in un trust point sul WLC, con questo comando: **echo | openssl s_client -connect**

  :443 -showcerts

  .

Nota: in questo modo viene generato un elenco dei certificati nella catena di attendibilità (con codifica PEM), quindi ogni certificato inizia con —BEGIN CERTIFICATE—. Fare riferimento all'URL indicato nella sezione Soluzione ed eseguire la procedura per configurare il certificato DNAC-CA, ma non importare il certificato CA radice. Importare invece il certificato della CA con problemi.

4.7.4. Certificato WLC scaduto.

- Quando la versione di Catalyst Center è 1.3.3.7 o precedente, il certificato WLC potrebbe essere scaduto. Se la versione di Catalyst Center è 1.3.3.8 o successiva (ma non la versione 2.1.2.6 o successiva), il problema può verificarsi anche se il certificato è scaduto prima dell'aggiornamento dalla versione 1.3.3.7 o precedente.
- Controllare la data di fine validità nell'output del **show crypto pki certificates sdn-network-infra-iwan** comando.

4.8. Il servizio Collector-Iosxe sul Catalyst Center non accetta la connessione dal WLC perché il servizio Inventory-Manager non ha notificato il nuovo dispositivo.

- Per controllare l'elenco delle periferiche conosciute da iosxe-collector, immettere questo comando dalla CLI di Catalyst Center:

  curl -s 'http://collector-iosxe-db.assurance-backend.svc.cluster.local:8077/api/internal/device/data'

- Per ottenere solo l'elenco dei nomi host e degli indirizzi IP, analizzare l'output con jq con

questo comando:

Su Catalyst Center versione 1.3 e successive:

curl -s 'http://collector-iosxe-db.assurance-backend.svc.cluster.local:8077/api/internal/device/data' | jq '.devices[] | .hostName, .mgmtIp'

Su Catalyst Center 1.3.1 e versioni precedenti:

curl -s 'http://collector-iosxe-db.assurance-backend.svc.cluster.local:8077/api/internal/device/data' | jq '.device[] | .hostName, .mgmtIp'

- Se l'elenco non contiene il WLC, riavviare il servizio Collector-Iosex e verificare se il problema è risolto.
- Se il riavvio di Collector-iosxe da solo non è utile, è possibile risolvere il problema riavviando il servizio di gestione del raccoglitore.

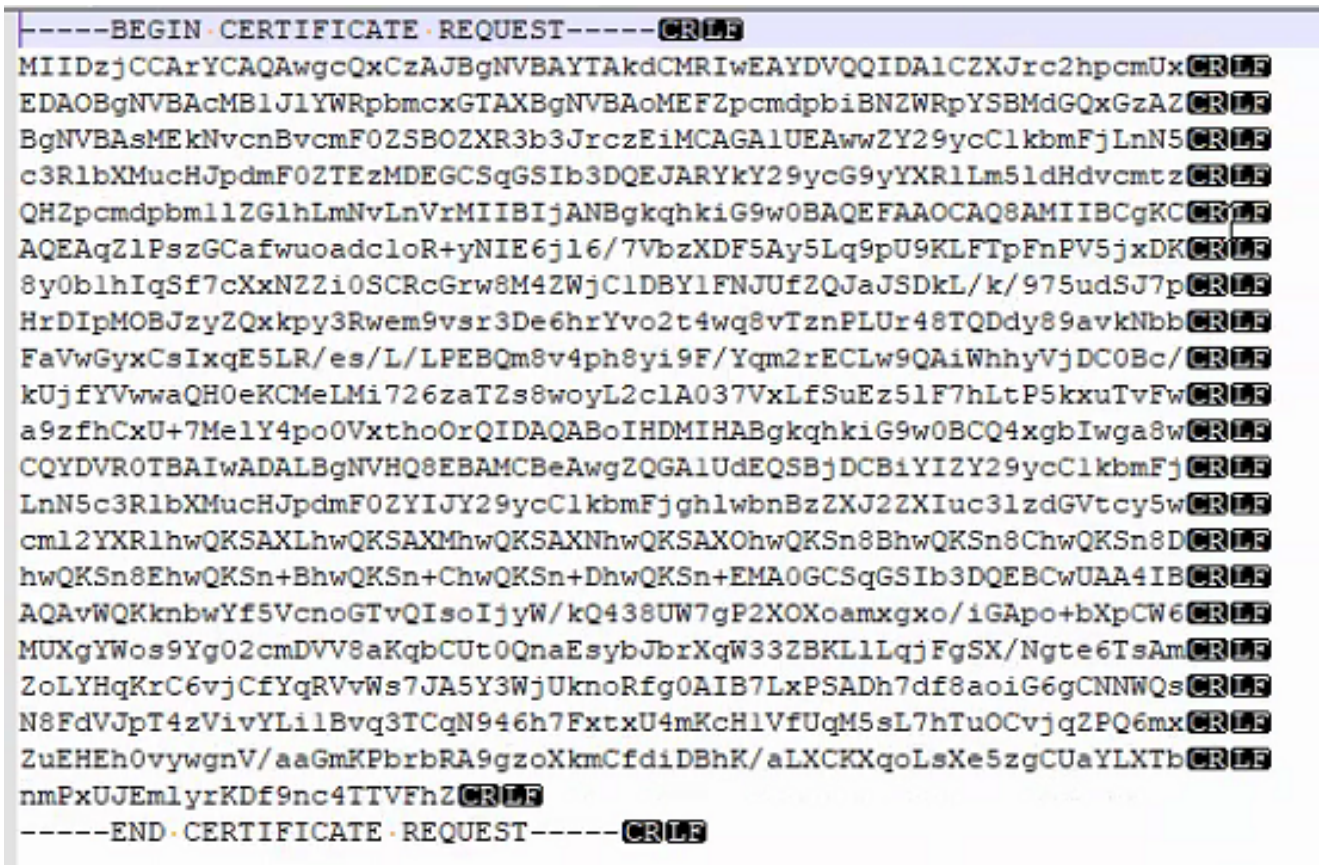
Suggerimento: per riavviare un servizio, immettere **magctl service restart -d** .

- Se l'output del comando **show telemetry internal connection** è ancora "Connecting"in esecuzione, eseguire la coda dei **collector-iosxe** log relativi all'errore:

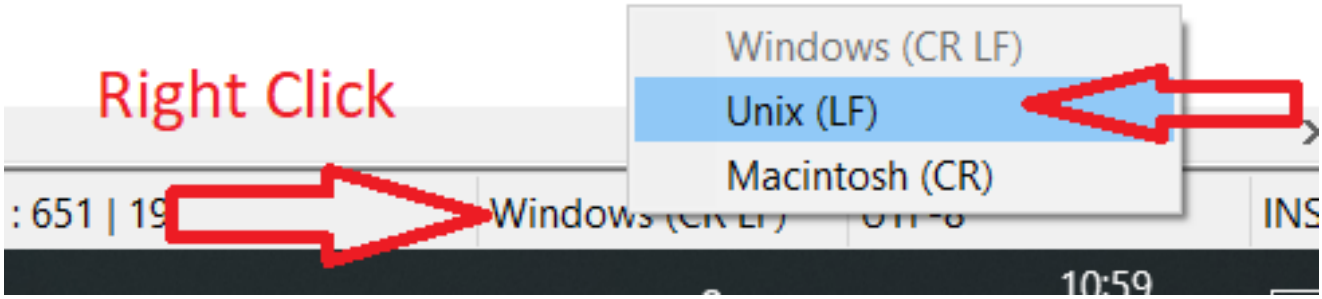
Suggerimento: per eseguire la coda di un file di log, immettere il **magctl service logs -rf** comando. In questo caso, **magctl service logs -rf collector-iosxe | lql**..

```
40 | 2021-04-29 08:09:15 | ERROR | pool-15-thread-1 | 121 | com.cisco.collector.ndp.common.KeyStor
      at java.util.Base64$Decoder.decode0(Base64.java:714)
```

- Se viene visualizzato questo errore, aprire il certificato aggiunto al Catalyst Center, i file con estensione key e pem (catena di certificati) in Blocco note++. In Blocco note++ passare a **View > Show Symbol > Show All Characters.**
- Se hai qualcosa del genere:



Andare quindi a:



Salvare i certificati.

- Aggiungerli nuovamente al Catalyst Center e verificare se il comando **show telemetry internal connection** viene visualizzato "Active".

4.9. Difetti correlati:

- ID bug Cisco CSCvs78950 - Connessione di telemetria del cluster WLC to Wolverine in stato 'Connecting'.
- Cisco bug ID CSCvr98535 - Cisco DNA Center non configura l'interfaccia di origine HTTP per PKI - la telemetria WLC rimane 'Connecting' (Connessione in corso).

Passaggio 5. Lo stato di telemetria è attivo, ma in Assurance non viene visualizzato alcun dato.

Verificare lo stato corrente della connessione interna di telemetria con questo comando:

```
<#root>

dna-9800#

show telemetry internal connection


Telemetry connection

Address          Port   Transport   State          Profile
-----------------------------------------------------------------
X.X.X.X       25103  tls-native

Active

        sdn-network-infra-iwan
```

Possibili difetti:

- Cisco bug ID CSCvu27838 - Nessun dato sulla garanzia wireless da 9300 con eWLC.
- Cisco bug ID CSCvu00173 - Route dell'API Assurance non registrata dopo l'aggiornamento alla versione 1.3.3.4 (non specifico di eWLC).

Soluzione alternativa

Se la configurazione richiesta o parte di essa non è presente nel WLC, provare a determinare la causa della mancata presenza della configurazione. Se esiste una corrispondenza per un difetto, controllare i file di registro pertinenti. Quindi, considerare queste opzioni come una soluzione alternativa.

Catalyst Center versione 2.x

Nell'interfaccia utente di Catalyst Center, passare alla **Inventory** pagina. Scegliere il **WLC** > **Actions** > **Telemetry** > **Update Telemetry Settings** > **Force Configuration Push** > **Next** > **Apply**pulsante. Successivamente, attendere qualche istante fino al termine del processo di risincronizzazione da parte del WLC. Verificare che Catalyst Center esegua il push della configurazione indicata nella sezione Informazioni di base di questo documento e che la configurazione Assurance sia presente sul WLC con il **show network-assurance summary** comando.

Catalyst Center versione 1.x

Questa opzione può essere utilizzata anche per Catalyst Center 2.x se il metodo GUI precedente non produce ancora l'effetto desiderato.

- Manca il sdn-network-infra-iwan trust point e/o il certificato.

Per installare manualmente i certificati e le sottoscrizioni Catalyst Center Assurance, contattare il Cisco Technical Assistance Center (TAC).

- La configurazione di Network Assurance non è presente.

  Verificare che l'indirizzo VIP dell'organizzazione del Catalyst Center sia raggiungibile dal WLC. Configurare quindi manualmente la sezione come illustrato nell'esempio seguente:

```
conf t
network-assurance url https://X.X.X.X
network-assurance icap server port 32626
network-assurance enable
network-assurance na-certificate PROTCOL_HTTP X.X.X.X /ca/ pem
```

Nota: sulla quinta riga, notare lo spazio tra X.X.X.X e /ca/ e lo spazio tra /ca/ e pem.

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).