Troubleshoot no Assurance Data in WLC 9800 on Catalyst Center

Contents

Introduction

This document describes how to troubleshoot when Cisco Catalyst Center does not show any Assurance data for a Catalyst 9800 Series WLC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Use of the Catalyst Center maglev CLI
- Basic Linux foundation
- Knowledge of certificates on Catalyst Center and on the Catalyst 9800 platform

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst Center appliance 1st or 2nd generation with software version 1.x or 2.x with Assurance package
- Catalyst 9800 Series Wireless LAN Controller (WLC)

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. If your network is live, ensure that you understand the potential impact of any command.

Note: While this document was initially written for Catalyst Center 1.x, most of it is valid for Catalyst Center 2.x.

Note: The Catalyst 9800 WLC must be already discovered by Catalyst Center and assigned to a site, and must run a compatible Cisco IOS® XE version. For more details about interoperability, refer to the Catalyst Center Compatibility Matrix.

Background Information

At the moment of the discovery process, Catalyst Center pushes the next configuration to the WLC.

Note: This example is from a Catalyst 9800-CL Cloud Wireless Controller. Some details can differ when you use a physical Catalyst 9800 Series appliance; X.X.X.X is the Virtual IP (VIP) address of the Catalyst Center enterprise interface and Y.Y.Y.Y is the management IP address of the 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
```

Troubleshoot No Assurance Data from WLC on Catalyst Center

Step 1. Verify that the WLC is reachable and managed in the Catalyst Center inventory.

If the WLC is not in Managed status, you must fix the reachability or provision issue before you continue.

> **Tip**: Check the inventory-manager, spf-device-manager, and spf-service-manager logs in order to identify the failure.

Step 2. Verify that Catalyst Center pushes all the necessary configurations to the WLC.

Ensure the configuration mentioned in the Background Information section was pushed to the WLC with these commands:

```
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
```

Known issues:

- Cisco bug ID CSCvs62939 - Cisco DNA Center does not push telemetry config to 9xxx switches after discovery.
- Cisco bug ID CSCvt83104 - eWLC Assurance config push failure if Netconf candidate datastore exists on the device.
- Cisco bug ID CSCvt97081 - eWLC DNAC-CA certificate provisioning fails for device discovered by DNS name.

Logs to verify:

- dna-wireless-service - for DNAC-CA certificate and telemetry configuration.
- network-design-service - for sdn-network-infra-iwan certificate.

Step 3. Verify that the necessary certificates get created on the WLC.

Ensure that the certificates get created correctly on WLC with these commands:

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

Known issues and limitations:

- Cisco bug ID CSCvu03730 - eWLC is unmonitored in Cisco DNA Center because the sdn-network-infra-iwan certificate is not installed (the root cause is that the pki-broker client cert is expired).
- Cisco bug ID CSCvr44560 - ENH: Add support for CA certificates expiring after 2099 for IOS-XE
- Cisco bug ID CSCwc99759 - ENH: Add support for 8192-bit RSA Certificate Signature

Step 4. Verify the telemetry connection status.

Ensure that the telemetry connection is in the Active state on the WLC with this command:

```
<#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
```

Or from Cisco IOS XE Release 17.7 and later:

```
<#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
```

The X.X.X.X IP address must be the Catalyst Center Enterprise interface. If Catalyst Center is configured with VIPs, this must be the VIP of the Enterprise interface. If the IP address is correct and the state is Active, proceed to the next step.

If the state is Connecting, then the Hypertext Transfer Protocol Secure (HTTPS) connection from the WLC to Catalyst Center was not established successfully. There can be many different reasons for this, the most common are listed next.

4.1. The Catalyst Center VIP is not reachable from the WLC or is in DOWN status.

- On a single node with VIP, the VIP goes down when the cluster interface goes down. Verify that the cluster interface is connected.
- Verify that the WLC has connectivity to the Enterprise VIP (ICMP/ping).
- Verify that the Catalyst Center Enterprise VIP is in the UP state, with this command: **ip a | grep en**.
- Verify that the Catalyst Center Enterprise VIP is properly configured with this command: **etcdctl get /maglev/config/cluster/cluster_network**.

4.2. The WLC is in High Availability (HA); Assurance does not work after failover.

This can occur if the HA is not formed by the Catalyst Center. In that case: remove the WLC from Inventory, break the HA, discover both WLCs, and let Catalyst Center form the HA.

Note: This requirement can change in later Catalyst Center versions.

4.3. Catalyst Center did not create the DNAC-CA trustpoint and certificate.

- Check Step 2 and Step 3 to fix this problem.

4.4. Catalyst Center did not create the sdn-network-infra-iwan trustpoint and certificate.

- Check Step 2 and Step 3 to fix this problem.

4.5. Catalyst Center did not push the Assurance configuration.

- The command **show network-assurance summary** shows Network-Assurance as **Disabled**:

<#root>

```
DC9800-WLC#

show network-assurance summary

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

Disabled

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

- Ensure the WLC has Device Controllability enabled, as this is required for Catalyst Center to push the configuration. Device Controllability can be enabled in the Discovery process, or once the WLC is on the Inventory and managed by Catalyst Center. Navigate to the **Inventory** page. Select **Device > Actions > Inventory > Edit Device > Device Controllability > Enable**.

4.6. Catalyst Center does not push the telemetry subscription configuration.

- Ensure that the WLC has the subscriptions with the **show telemetry ietf subscription all** command.
- If not, check Step 2 and Step 3 in order to fix this problem.

4.7. The TLS handshake between the WLC and Catalyst Center fails because the Catalyst Center certificate cannot be validated by the WLC.

This could be due to many reasons, the most common ones are listed here:

4.7.1. The Catalyst Center certificate is expired, or revoked, or does not have the Catalyst Center IP address in the Subject Alternate Name (SAN).

- Ensure the certificate matches the best practices specified in the Catalyst Center Security Best Practices Guide.

4.7.2. The revocation check fails because the Certificate Revocation List (CRL) cannot be retrieved.

- There can be many reasons for the CRL retrieval to fail; such as a DNS failure, firewall issue, connectivity issue between the WLC and the CRL Distribution Point (CDP), or one of these known issues:
  - Cisco bug ID CSCvr41793 - PKI: CRL retrieval does not use HTTP Content-Length.
  - Cisco bug ID CSCvo03458 - PKI, revocation check crl none, does not fallback if CRL is not reachable.
  - Cisco bug ID CSCue73820 - PKI debugs not clear about CRL parse failure.
- As a workaround, configure revocation-check none under the DNAC-CA trustpoint.

4.7.3. Certificate error "Peer certificate chain is too long to be verified".

- Check the output from the **show platform software trace message mdt-pubd chassis active R** command.
- If this shows **"Peer certificate chain is too long to be verified"** then check:

  Cisco bug ID CSCvw09580 - 9800 WLC does not take Cisco DNA Center certificate chains depth with 4 and more.

- In order to fix this, import the certificate of the intermediate CA that issued the Catalyst Center certificate, into a trustpoint on the WLC, with this command: **echo | openssl s_client -connect <Catalyst Center IP>:443 -showcerts.**

Note: This produces a list of the certificates in the trust chain (PEM encoded), so each certificate starts with -----BEGIN CERTIFICATE-----. Refer to the URL mentioned in the Workaround section, and execute the steps to configure the DNAC-CA certificate, but do not import the root CA certificate. Instead, import the certificate of the problematic CA.

4.7.4. WLC certificate expired.

- When the Catalyst Center version is 1.3.3.7 or earlier, the WLC certificate could have expired. When the Catalyst Center version is 1.3.3.8 or later (but not 2.1.2.6 or later) then this can still be an issue if the certificate expired before the upgrade from Version 1.3.3.7 or earlier.
- Check the validity end date in the output of the **show crypto pki certificates sdn-network-infra-iwan** command.

4.8. The collector-iosxe service on Catalyst Center does not accept the connection from the WLC because it was not notified of the new device by the inventory-manager service.

- In order to check the list of devices known by iosxe-collector, enter this command on the Catalyst

Center CLI:

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

- In order to get just the list of hostnames and IP addresses, parse the output with jq with this command:

  On Catalyst Center 1.3 and later:

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

  On Catalyst Center 1.3.1 and earlier:

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

- If this list does not contain the WLC, then restart the collector-iosxe service and confirm whether this solves the issue.
- If a restart of collector-iosxe alone does not help, a restart of the collector-manager service can help to solve this issue.

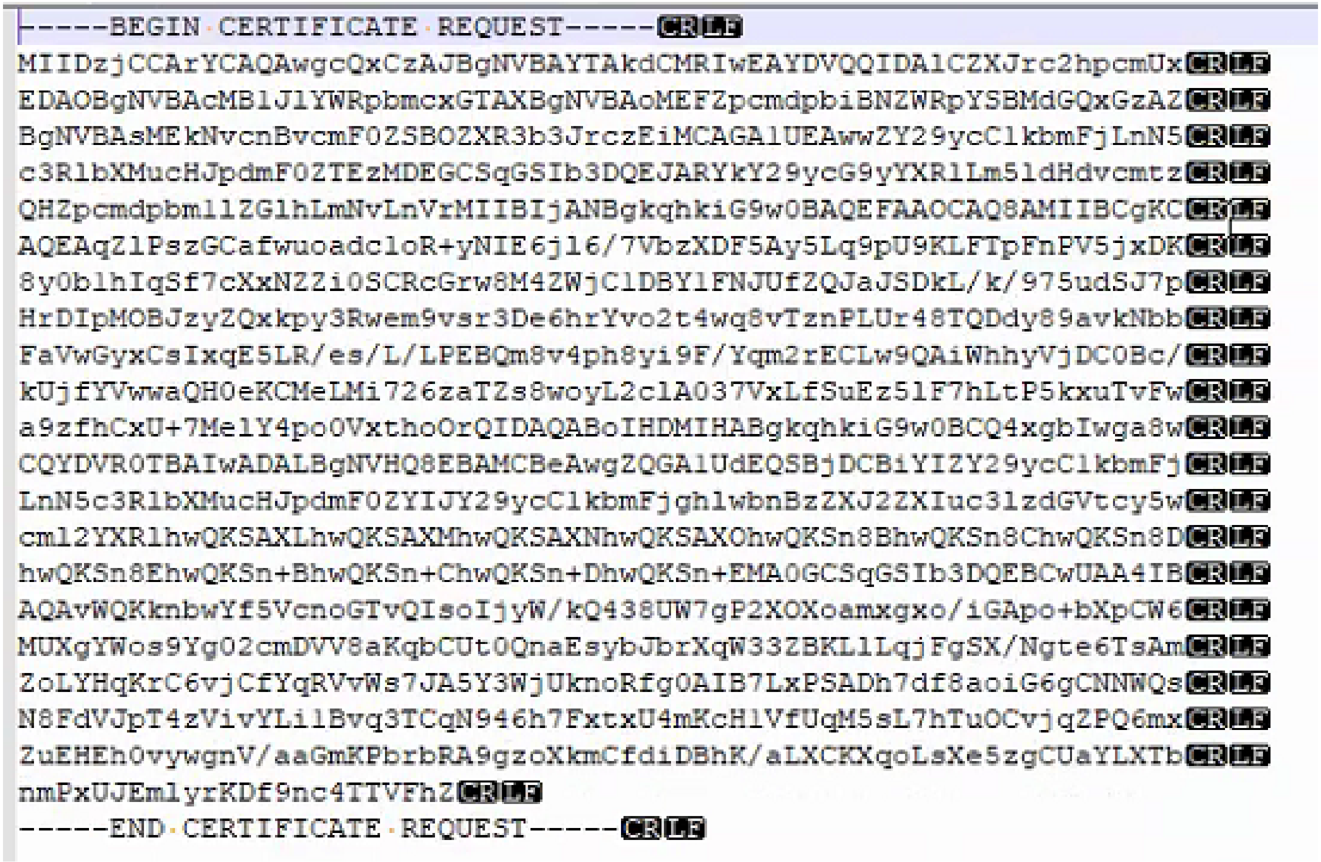
Tip: In order to restart a service, enter **magctl service restart -d <service_name>.**

- If the output of the command **show telemetry internal connection** is still Connecting, tail the **collector-iosxe** logs for the error:

Tip: In order to tail a log file, enter the **magctl service logs -rf <service_name>** command. In this case, **magctl service logs -rf collector-iosxe | lql**..

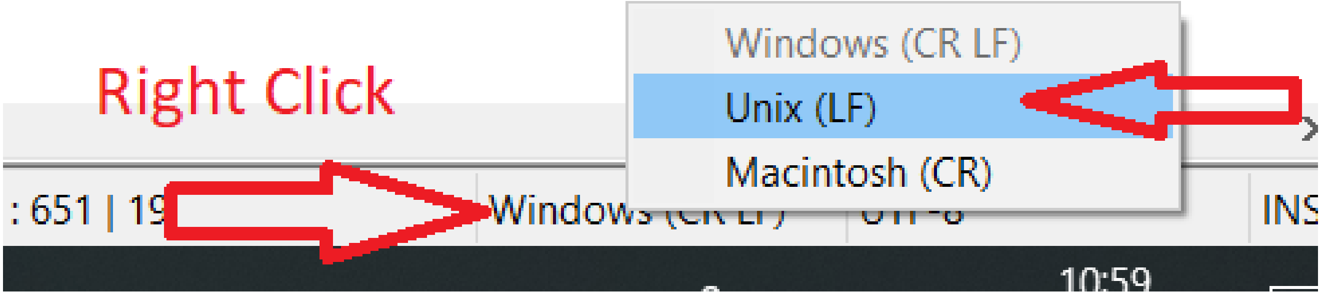
```
40 | 2021-04-29 08:09:15 | ERROR | pool-15-thread-1 | 121 | com.cisco.collector.ndp.common.KeyStor
      at java.util.Base64$Decoder.decode0(Base64.java:714)
```

- If you see this error, then open the certificate which was added to the Catalyst Center, both its .key and .pem (certificate chain) files in Notepad++. In Notepad++, navigate to **View** > **Show Symbol** > **Show All Characters**.
- If you have something like this:



```
-----BEGIN CERTIFICATE REQUEST----- CR LF
MIIDzjCCArYCAQAwgcQxCzAJBgNVBAYTAkdCMRIwEAYDVQQIDA1CZXJrc2hpcmUx CR LF
EDAOBgNVBAcMB1J1YWRpbmcxGTAXBgNVBAoMEFZpcmdpbiBNZWRpYSBMdGQxGzAZ CR LF
BgNVBAsMEkNvcnBvcmF0ZSBOZXR3b3JrczEiMCAGA1UEAwwZY29ycC1kbmFjLnN5 CR LF
c3RlbXMucHJpdmF0ZTEzMDEGCSqGSIb3DQEJARYkY29ycG9yYXRlLm51dHdvcmtz CR LF
QHZpcmdpbm11ZGlhLmNvLnVrMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC CR LF
AQEAqZ1PszGCafwuoadcloR+yNIE6jl6/7VbzXDF5Ay5Lq9pU9KLFTpFnPV5jxDK CR LF
8y0blhIqSf7cXxNZZi0SCRcGrw8M4ZWjC1DBY1FNJUfZQJaJSDkL/k/975udSJ7p CR LF
HrDIpMOBJzyZQxkpy3Rwem9vsr3De6hrYvo2t4wq8vTznPLUr48TQDdy89avkNbb CR LF
FaVwGyxCsIxqE5LR/es/L/LPEBQm8v4ph8yi9F/Yqm2rECLw9QAiWhhyVjDC0Bc/ CR LF
kUjfYVwwaQH0eKCMeLMi726zaTZs8woyL2clA037VxLfSuEz51F7hLtP5kxuTvFw CR LF
a9zfhCxU+7Me1Y4po0VxthoOrQIDAQABoIHDMIHABgkqhkiG9w0BCQ4xgbIwga8w CR LF
CQYDVR0TBAIwADALBgNVHQ8EBAMCBeAwgZQGA1UdEQSBjDCBiYIZY29ycC1kbmFj CR LF
LnN5c3RlbXMucHJpdmF0ZYIJY29ycC1kbmFjghlwbnBzZXJ2ZXIuc3lzdGVtcy5w CR LF
cml2YXRlhwQKSAXLhwQKSAXMhwQKSAXNhwQKSAXOhwQKSn8BhwQKSn8ChwQKSn8D CR LF
hwQKSn8EhwQKSn+BhwQKSn+ChwQKSn+DhwQKSn+EMA0GCSqGSIb3DQEBCwUAA4IB CR LF
AQAvWQKknbwYf5VcnoGTvQIsoIjyW/kQ438UW7gP2XOXoamxgxo/iGApo+bXpCW6 CR LF
MUXgYWos9Yg02cmDVV8aKqbCUt0QnaEsybJbrXqW33ZBKL1LqjFgSX/Ngte6TsAm CR LF
ZoLYHqKrC6vjCfYqRVvWs7JA5Y3WjUknoRfg0AIB7LxPSADh7df8aoiG6gCNNWQs CR LF
N8FdVJpT4zVivYLi1Bvq3TCqN946h7FxtxU4mKcH1VfUqM5sL7hTuOCvjqZPQ6mx CR LF
ZuEHEh0vywgnV/aaGmKPbrbRA9gzoXkmCfdiDBhK/aLXCKXqoLsXe5zgCUaYLXTb CR LF
nmPxUJEmlyrKDf9nc4TTVFhZ CR LF
-----END CERTIFICATE REQUEST----- CR LF
```

Then navigate to:



And save the certificates.

- Add them again to the Catalyst Center and check if the **show telemetry internal connection** command now shows Active.

4.9. Related defects:

- Cisco bug ID CSCvs78950 - eWLC to Wolverine cluster telemetry connection in Connecting state.
- Cisco bug ID CSCvr98535 - Cisco DNA Center does not configure HTTP source interface for PKI - eWLC telemetry stays Connecting.

Step 5. The telemetry state is active, but still, no data is seen in Assurance.

Verify the current status of the telemetry internal connection with this command:

<#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
```

Possible defects:

- Cisco bug ID CSCvu27838 - No wireless assurance data from 9300 with eWLC.
- Cisco bug ID CSCvu00173 - Assurance API route not registered after upgrade to 1.3.3.4 (not specific to eWLC).

Workaround

If some or all of the required configuration is not in the WLC, try to determine why the configuration is not present. Check the relevant log files if there is a match for a defect. After that, consider these options as a workaround.

Catalyst Center Version 2.x

On the Catalyst Center GUI, navigate to the **Inventory** page. Choose the **WLC** > **Actions** > **Telemetry** > **Update Telemetry Settings** > **Force Configuration Push** > **Next** > **Apply**.After that, wait some time until the WLC finishes the resynchronization process. Verify that Catalyst Center pushes the configuration mentioned in the Background Information section of this document and verify that the Assurance configuration is present on the WLC with the **show network-assurance summary** command.

Catalyst Center Version 1.x

This can also be used for Catalyst Center 2.x if the previous GUI method still does not have the desired effect.

- The sdn-network-infra-iwan trustpoint and/or certificate is missed.

  Contact the Cisco Technical Assistance Center (TAC) in order to manually install the Catalyst Center Assurance certificates and subscriptions.

- Network-assurance configuration is not present.

  Ensure the Catalyst Center enterprise VIP address is reachable from the WLC. Then configure the section manually as shown in the next example:

```
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
```

Note: On the fifth line, note the space between X.X.X.X and /ca/ and also the space between /ca/ and pem.