# Fehlerbehebung bei "No Assurance Data" im WLC 9800 auf Cisco DNA Center

## Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[Fehlerbehebung: Keine Assurance-Daten von WLC im Cisco DNA Center](#)
[Problemumgehung](#)
[Cisco DNA Center Version 2.x](#)
[Cisco DNA Center Version 1.x](#)

## Einleitung

In diesem Dokument wird die Fehlerbehebung beschrieben, wenn Cisco DNA Center keine Assurance-Daten für einen Catalyst Wireless LAN Controller (WLC) der Serie 9800 anzeigt.

---

> **Hinweis**: Dieses Dokument wurde ursprünglich für Cisco DNA Center 1.x verfasst, deckt jedoch größtenteils Cisco DNA Center 2.x ab.

---

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Nutzung des Cisco DNA Center maglev CLI
- Grundlegende Linux-Grundlagen
- Kenntnisse über Zertifikate im Cisco DNA Center und auf der Cisco Catalyst 9800-Plattform

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco DNA Center Appliance 1. oder 2. Generation mit Softwareversion 1.x oder 2.x mit Assurance-Paket
- Cisco Catalyst WLC der Serie 9800

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

---

> **Hinweis**: Der Catalyst 9800 WLC muss von Cisco DNA Center erkannt und einem Standort

---

zugewiesen worden sein sowie mit einer kompatiblen Cisco IOS® XE-Version betrieben werden. Weitere Informationen zur Interoperabilität finden Sie in der Kompatibilitätsmatrix für Cisco DNA Center.

# Hintergrundinformationen

Zum Zeitpunkt des Erkennungsprozesses überträgt das Cisco DNA Center die nächste Konfiguration an den WLC.

**Hinweis**: Dieses Beispiel stammt von einem Cisco Catalyst 9800-CL Cloud Wireless Controller. Einige Details können sich unterscheiden, wenn Sie eine physische Appliance der Cisco Catalyst Serie 9800 verwenden: X.X.X.X ist die virtuelle IP (VIP)-Adresse der Cisco DNA Center Enterprise-Schnittstelle, und Y.Y.Y.Y ist die Management-IP-Adresse des 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 Cisco DNA 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
```

# Fehlerbehebung: Keine Assurance-Daten von WLC im Cisco DNA Center

Schritt 1: Überprüfen der Erreichbarkeit und Verwaltung des WLC im Cisco DNA Center-Inventar

Wenn der WLC nicht den Status "Verwaltet" hat, müssen Sie das Problem mit der Erreichbarkeit oder die Bereitstellung beheben, bevor Sie fortfahren.

---

> **Tipp:** Überprüfen Sie die Protokolle "Inventory-manger", "spf-device-manager" und "spf-service-manager", um den Fehler zu identifizieren.

---

Schritt 2: Vergewissern Sie sich, dass das Cisco DNA Center alle erforderlichen Konfigurationen an den WLC übermittelt.

Stellen Sie sicher, dass die im Abschnitt Background Information (Hintergrundinformationen) erwähnte Konfiguration mithilfe der folgenden Befehle an den WLC gesendet wurde:

```
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
```

Bekannte Probleme:

- Cisco Bug-ID CSCvs62939 - Cisco DNA Center übermittelt Telemetriekonfiguration auf 9xxx-Switches nach der Erkennung nicht.
- Cisco Bug-ID CSCvt83104 - eWLC Assurance-Konfiguration Push-Fehler, wenn Netconf-Kandidatendatendatenspeicher auf dem Gerät vorhanden ist.
- Cisco Bug-ID CSCvt97081 - eWLC DNAC-CA-Zertifikatbereitstellung für Gerät, das vom DNS-Namen erkannt wurde, fehlgeschlagen.

Protokolle zur Überprüfung:

- dna-wireless-service - für DNAC-CA-Zertifikat und Telemetriekonfiguration.
- network-design-service - für das sdn-network-infra-iwan-Zertifikat.

Schritt 3: Stellen Sie sicher, dass die erforderlichen Zertifikate auf dem WLC erstellt werden.

Stellen Sie mit den folgenden Befehlen sicher, dass die Zertifikate auf dem WLC richtig erstellt werden:

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

Bekanntes Problem:

- Cisco Bug-ID CSCvu03730 - eWLC wird im Cisco DNA Center nicht überwacht, da das sdn-network-infra-iwan-Zertifikat nicht installiert ist (Ursache ist, dass das pki-broker-Client-Zertifikat abgelaufen ist).

Schritt 4: Überprüfen Sie den Status der Telemetrie-Verbindung.

Stellen Sie sicher, dass sich die Telemetrieverbindung im "Active" mit dem folgenden Befehl auf dem WLC:

```
<#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
```

oder ab Cisco IOS XE Version 17.7:

```
<#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
```

Bei der X.X.X.X-IP-Adresse muss es sich um die Cisco DNA Center Enterprise-Schnittstelle handeln. Wenn Cisco DNA Center mit VIPs konfiguriert ist, muss dies das VIP der Enterprise-Schnittstelle sein. Wenn die IP-Adresse richtig ist und der Status "Active", fahren Sie mit dem nächsten Schritt fort.

Wenn der Status "Connecting" konnte die sichere Hypertext Transfer Protocol (HTTPS)-Verbindung vom WLC zum Cisco DNA Center nicht erfolgreich hergestellt werden. Es kann viele verschiedene Gründe dafür geben, die häufigsten werden als Nächstes aufgelistet.

4.1. Das Cisco DNA Center VIP ist vom WLC aus nicht erreichbar oder "DOWN" status.

- Auf einem einzelnen Knoten mit VIP fällt das VIP aus, wenn die Cluster-Schnittstelle ausfällt. Überprüfen Sie, ob die Cluster-Schnittstelle angeschlossen ist.
- Überprüfen Sie, ob der WLC über eine Verbindung zum Enterprise VIP (ICMP/Ping) verfügt.
- Überprüfen Sie, ob das Cisco DNA Center Enterprise VIP im "UP" state (Status) mit dem folgenden Befehl: **ip a | grep en.**
- Stellen Sie sicher, dass Cisco DNA Center Enterprise VIP mit dem folgenden Befehl ordnungsgemäß konfiguriert ist: **etcdctl get /maglev/config/cluster/cluster_network.**

4.2. Der WLC befindet sich in Hochverfügbarkeit (HA), Assurance funktioniert nach Failover nicht.

Dies kann der Fall sein, wenn die HA nicht vom Cisco DNA Center gebildet wurde. In diesem Fall: Entfernen Sie den WLC aus dem Bestand, unterbrechen Sie die HA-Stufe, entdecken Sie beide WLCs, und lassen Sie das Cisco DNA Center die HA-Stufe bilden.

---

**Hinweis**: Diese Anforderung kann sich in späteren Versionen von Cisco DNA Center ändern.

---

4.3. Cisco DNA Center hat den DNAC-CA-Vertrauenspunkt und das -Zertifikat nicht erstellt.

- Überprüfen Sie die Schritte 2 und 3, um dieses Problem zu beheben.

4.4 Das Cisco DNA Center hat die sdn-network-infra-iwan Trustpoint und Zertifikat.

- Überprüfen Sie die Schritte 2 und 3, um dieses Problem zu beheben.

4.5. Cisco DNA Center hat die Assurance-Konfiguration nicht weiterentwickelt.

- Der Befehl **show network-assurance summary** zeigt Network Assurance als **Disabled**:

```
<#root>

DC9800-WLC#

show network-assurance summary

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

Disabled

Server Url                           :
ICap Server Port Number           :
```

```
Sensor Backhaul SSID                  :
Authentication                        : Unknown
```

- Stellen Sie sicher, dass die Gerätesteuerung auf dem WLC aktiviert ist, da dies erforderlich ist, damit Cisco DNA Center die Konfiguration vorantreiben kann. Die Gerätesteuerung kann im Ermittlungsprozess oder nachdem der WLC im Bestand vorhanden ist und vom Cisco DNA Center verwaltet wird, aktiviert werden. Navigieren Sie zum **Inventory** Seite. Wählen Sie **device > Actions > Inventory > Edit Device > Device Controllability > Enable.**

4.6. Cisco DNA Center überträgt die Konfiguration des Telemetrie-Abonnements nicht.

- Stellen Sie sicher, dass der WLC über die Abonnements mit dem **show telemetry ietf subscription all** aus.
- Wenn nicht, überprüfen Sie die Schritte 2 und 3, um dieses Problem zu beheben.

4.7. Der TLS-Handshake zwischen WLC und Cisco DNA Center schlägt fehl, da das Cisco DNA Center-Zertifikat vom WLC nicht validiert werden kann.

Dies kann auf viele Gründe zurückzuführen sein, die häufigsten sind hier aufgeführt:

4.7.1. Das Cisco DNA Center-Zertifikat ist abgelaufen oder widerrufen oder weist die Cisco DNA Center-IP-Adresse nicht im Subject Alternate Name (SAN) auf.

- Stellen Sie sicher, dass das Zertifikat mit den Best Practices im Cisco DNA Center Security Best Practices Guide übereinstimmt.

4.7.2. Die Sperrprüfung schlägt fehl, da die Zertifikatsperrliste (Certificate Revocation List, CRL) nicht abgerufen werden kann.

- Der CRL-Abruf kann aus verschiedenen Gründen fehlschlagen, z. B. aufgrund eines DNS-Fehlers, eines Firewall-Problems, eines Verbindungsproblems zwischen dem WLC und dem CRL Distribution Point (CDP) oder eines der folgenden bekannten Probleme:
  - Cisco Bug-ID CSCvr41793 - PKI: Beim CRL-Abruf wird die HTTP-Inhaltslänge nicht verwendet.
  - Cisco Bug-ID CSCvo03458 - PKI "revocation check crl none" fällt nicht zurück, wenn CRL nicht erreichbar ist.
  - Cisco Bug-ID CSCue73820 - PKI debuggt nicht eindeutig über Fehler beim Analysieren von Zertifikatsperrlisten.
- Konfigurieren Sie als Workaround **revocation-check none** unter dem DNAC-CA-Vertrauenspunkt.

4.7.3. Zertifikatfehler "Die Zertifikatkette des Peers ist zu lang, um überprüft zu werden".

- Prüfen Sie die Ausgabe des **show platform software trace message mdt-pubd chassis active R** aus.
- Wenn dies angezeigt wird **"Peer certificate chain is too long to be verified"** dann prüfen:

  Cisco Bug-ID CSCvw09580 - 9800 WLC nimmt keine Cisco DNA Center-Zertifikatkettentiefe mit 4 und mehr an.

- Importieren Sie dazu das Zertifikat der zwischengeschalteten Zertifizierungsstelle, die das Cisco DNA Center-Zertifikat ausgestellt hat, mit dem folgenden Befehl in einen Vertrauenspunkt auf dem WLC: **echo | openssl s_client -connect**

  **:443 -showcerts**

  .

**Hinweis**: Dadurch wird eine Liste der Zertifikate in der Vertrauenskette (PEM-codiert) erstellt, sodass jedes Zertifikat mit -----BEGIN CERTIFICATE----- beginnt. Gehen Sie zu der URL, die im Abschnitt Problemumgehung erwähnt wird, und führen Sie die Schritte aus, um das DNAC-CA-Zertifikat zu konfigurieren. Importieren Sie jedoch nicht das Stamm-CA-Zertifikat. Importieren Sie stattdessen das Zertifikat der problematischen Zertifizierungsstelle.

4.7.4. WLC-Zertifikat abgelaufen.

- Wenn die Cisco DNA Center-Version 1.3.3.7 oder älter ist, kann das WLC-Zertifikat abgelaufen sein. Wenn die Version 1.3.3.8 oder höher von Cisco DNA Center (jedoch nicht 2.1.2.6 oder höher) verwendet wird, kann dies immer noch ein Problem darstellen, wenn das Zertifikat vor dem Upgrade von Version 1.3.3.7 oder höher abgelaufen ist.
- Überprüfen Sie das Gültigkeitsenddatum in der Ausgabe des **show crypto pki certificates sdn-network-infra-iwan** aus.

4.8. Der Collector-Iosxe-Service im Cisco DNA Center akzeptiert die Verbindung vom WLC nicht, da er vom Inventar-Manager-Service nicht über das neue Gerät informiert wurde.

- Um die Liste der von iosxe-collection bekannten Geräte zu überprüfen, geben Sie den folgenden Befehl in die CLI von Cisco DNA Center ein:

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

- Um nur die Liste der Hostnamen und IP-Adressen zu erhalten, parsen Sie die Ausgabe mit dem folgenden Befehl mit jq:

  Cisco DNA Center 1.3 und höher:

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

  Cisco DNA Center 1.3.1 und frühere Versionen:

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

- Wenn diese Liste den WLC nicht enthält, starten Sie den Collector-Iosxe-Dienst neu, und überprüfen Sie, ob das Problem dadurch behoben wird.
- Wenn ein Neustart von Collector-iosxe allein nicht hilft, kann ein Neustart des Collector-Manager-Dienstes helfen, dieses Problem zu lösen.

  **Tipp:** Um einen Service neu zu starten, geben Sie Folgendes ein: **magctl service restart -d** .

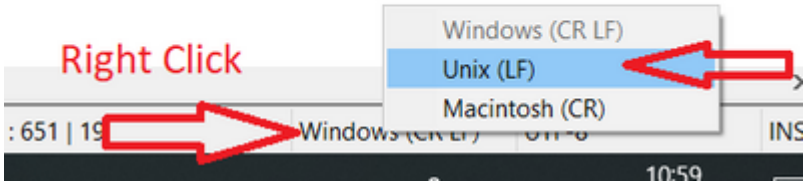
- Wenn die Ausgabe des Befehls **show telemetry internal connection** ist immer noch "Connecting", schwanzt **collector-iosxe** Protokolle für den Fehler:

  **Tipp:** Um eine Protokolldatei per Tail zu versenden, geben Sie den **magctl service logs -rf** aus. In diesem Fall **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.KeyStoreManager | java.lang.IllegalArgumentException: Exception setting server keystore
at java.util.Base64$Decoder.decode0(Base64.java:714)

- Wenn Sie diesen Fehler sehen, öffnen Sie das Zertifikat, das im Cisco DNA Center hinzugefügt wurde, sowohl die .key-Datei als auch die .pem-Datei (Zertifikatskette) im Notepad++. Navigieren Sie im Editor++ zu **View > Show Symbol > Show All Characters.**
- Wenn Sie so etwas haben:


Gehen Sie dann zu:




Speichern Sie die Zertifikate.

- Fügen Sie sie erneut im Cisco DNA Center hinzu, und überprüfen Sie, ob die **show telemetry internal connection** Befehl zeigt jetzt an "Active".

4.9. Verwandte Mängel:

- Cisco Bug-ID CSCvs78950 - eWLC-zu-Wolverine-Cluster-Telemetrieverbindung im Status "Connecting" (Verbinden).
- Cisco Bug-ID CSCvr98535 - Cisco DNA Center konfiguriert keine HTTP-Quellschnittstelle für PKI - eWLC-Telemetriedaten bleiben "Connecting".

Schritt 5: Der Telemetriestatus ist aktiv, aber in Assurance werden immer noch keine Daten angezeigt.

Überprüfen Sie mit dem folgenden Befehl den aktuellen Status der internen Telemetrieverbindung:

<#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
```

Mögliche Mängel:

- Cisco Bug-ID CSCvu27838 - Keine Wireless-Sicherungsdaten von 9300 mit eWLC.
- Cisco Bug-ID CSCvu00173 - Assurance-API-Route nach Upgrade auf 1.3.3.4 nicht registriert (nicht spezifisch für eWLC).

# Problemumgehung

Wenn sich einige oder alle der erforderlichen Konfigurationen nicht im WLC befinden, versuchen Sie festzustellen, warum die Konfiguration nicht vorhanden ist. Überprüfen Sie die entsprechenden Protokolldateien, wenn eine Übereinstimmung für einen Fehler vorliegt. Betrachten Sie diese Optionen anschließend als Problemumgehung.

## Cisco DNA Center Version 2.x

Navigieren Sie auf der Benutzeroberfläche von Cisco DNA Center zur **Inventory** Seite. Wählen Sie **WLC** > **Actions** > **Telemetry** > **Update Telemetry Settings** > **Force Configuration Push** > **Next** > **Apply**. Warten Sie danach einige Zeit, bis der WLC den Resynchronisierungsvorgang abgeschlossen hat. Stellen Sie sicher, dass Cisco DNA Center die im Abschnitt mit den Hintergrundinformationen genannte Konfiguration weiterleitet, und vergewissern Sie sich, dass die Assurance-Konfiguration auf dem WLC mit dem **show network-assurance summary** aus.

## Cisco DNA Center Version 1.x

Dies kann auch für Cisco DNA Center 2.x verwendet werden, wenn die bisherige GUI-Methode noch nicht die gewünschte Wirkung zeigt.

- Die Fehlermeldung sdn-network-infra-iwan Vertrauenspunkt und/oder Zertifikat fehlen.

  Wenden Sie sich an das Cisco Technical Assistance Center (TAC), um die Cisco DNA Center Assurance-Zertifikate und -Abonnements manuell zu installieren.

- Eine Konfiguration zur Netzwerksicherung ist nicht vorhanden.

  Stellen Sie sicher, dass die Cisco DNA Center Enterprise VIP-Adresse vom WLC aus erreichbar ist. Konfigurieren Sie den Abschnitt anschließend manuell, wie im folgenden Beispiel gezeigt:

```
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
```

**Hinweis**: Beachten Sie in der fünften Zeile den Abstand zwischen X.X.X.X und /ca/ sowie den Abstand zwischen /ca/ und pem.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.