

# Probleemoplossing zonder betrouwbaarheidsgegevens in WLC 9800 op Cisco DNA Center

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Probleemoplossing zonder betrouwbaarheidsgegevens van WLC op Cisco DNA Center](#)

[Tijdelijke oplossing](#)

[Cisco DNA Center versie 2.x](#)

[Cisco DNA Center versie 1.x](#)

## Inleiding

Dit document beschrijft hoe u problemen kunt oplossen wanneer Cisco DNA Center geen Assurance-gegevens toont voor een Catalyst 9800 Series draadloze LAN-controller (WLC).

---

**Opmerking:** terwijl dit document aanvankelijk was geschreven voor Cisco DNA Center 1.x, is het grootste deel ervan geldig voor Cisco DNA Center 2.x.

---

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Gebruik van het Cisco DNA Center maglev CLI
- Basic Linux foundation
- Kennis van certificaten op Cisco DNA Center en op het Cisco Catalyst 9800-platform

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco DNA Center-applicatie van de 1e of 2e generatie met softwareversie 1.x of 2.x met Assurance-pakket
- Cisco Catalyst 9800 Series WLC

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

---

**Opmerking:** de Catalyst 9800 WLC moet al door Cisco DNA Center worden ontdekt en aan een site worden toegewezen, en moet een compatibele Cisco IOS® XE-versie uitvoeren. Raadpleeg voor meer informatie over interoperabiliteit de [Cisco DNA Center-compatibiliteitsmatrix](#).

---

## Achtergrondinformatie

Op het ogenblik van het ontdekkingsproces, duwt Cisco DNA Center de volgende configuratie aan WLC.

---

**Opmerking:** dit voorbeeld komt uit een Cisco Catalyst 9800-CL draadloze controller voor de cloud. Sommige details kunnen verschillen wanneer u een fysiek Cisco Catalyst 9800 Series-apparaat gebruikt; X.X.X.X is het virtuele IP (VIP)-adres van de ondernemingsinterface van Cisco DNA Center en Y.Y.Y.Y is het IP-adres voor beheer van de 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
```

## Probleemoplossing zonder betrouwbaarheidsgegevens van WLC op Cisco DNA Center

Stap 1. Controleer dat de WLC bereikbaar is en wordt beheerd in de inventaris van Cisco DNA Center.

Als de WLC niet in Beheerde status is, moet u de bereikbaarheid of provisioningkwesitie oplossen voordat u doorgaat.

---

**Tip:** controleer de logbestanden inventaris-manager, spf-apparaat-manager en spf-service-manager om de fout te identificeren.

---

Stap 2. Controleer of Cisco DNA Center alle benodigde configuratie naar de WLC heeft gedrukt.

Zorg ervoor dat de configuratie zoals vermeld in de sectie Achtergrondinformatie met deze opdrachten naar de WLC is gedruwd:

```
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
```

Bekende problemen:

- Cisco bug-id [CSCvs62939](#) - Cisco DNA Center drukt telemetrieconfiguratie na detectie niet naar 900 switches.
- Cisco bug-id [CSCvt83104](#) - WLC-betrouwbaarheidsconfiguratiefouten als NetConf-kandidaat-datastore op apparaat bestaat.
- Cisco bug-id [CSCvt97081](#) - WLC DNAC-CA certificaatprovisioning mislukt voor apparaat ontdekt door DNS-naam.

Te verifiëren logbestanden:

- DNA-Wireless-Service - voor DNAC-CA certificaat- en telemetrieconfiguratie.
- Network-Design-Service - voor SDN-Network-infra-iwan-certificaat.

Stap 3. Controleer dat de benodigde certificaten op de WLC worden gemaakt.

Zorg ervoor dat de certificaten correct op WLC met deze opdrachten worden gemaakt:

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

Bekende kwestie:

- Cisco bug-id [CSCvu03730](#) - eWLC is niet gemonitord in Cisco DNA Center omdat het ISDN-netwerk-infra-iwan certificaat niet is geïnstalleerd (oorzaak is dat de client-cert van de pki-broker is verlopen).

Stap 4. Controleer de status van de telemetrieverbinding.

Zorg ervoor dat de telemetrieverbinding in de "Active" de staat op WLC met dit bevel:

```
<#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
```

Of van Cisco IOS XE release 17.7 en hoger:

```
<#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

Het X.X.X.X IP-adres moet de interface van Cisco DNA Center Enterprise zijn. Als Cisco DNA Center met VIPâ€™s is geconfigureerd, moet dit de VIP van de Enterprise-interface zijn. Als het IP-adres juist is en de status "Active", gaat u verder naar de volgende stap.

Indien de staat "Connecting" vervolgens is de HTTPS-verbinding (Hypertext Transfer Protocol Secure) van de WLC naar Cisco DNA Center niet tot stand gebracht. Er kunnen veel verschillende redenen voor zijn, de meest voorkomende zijn hieronder vermeld.

4.1. De VIP van Cisco DNA Center is niet bereikbaar via de WLC of is niet beschikbaar in "DOWN" status.

- Op één knooppunt met VIP gaat de VIP naar beneden wanneer de clusterinterface naar beneden gaat. Controleer of de clusterinterface is verbonden.
- Controleer of de WLC verbinding heeft met de Enterprise VIP (ICMP/ping).
- Controleer of de VIP van Cisco DNA Center Enterprise in de "UP" staat, met dit bevel: `ip a | grep en`.
- Controleer of de VIP van Cisco DNA Center Enterprise met deze opdracht correct is geconfigureerd: `etcdctl get /maglev/config/cluster/cluster_network`.

4.2. De WLC is in High Availability (HA), Assurance werkt niet na failover.

Dit kan voorkomen als de HA niet is gevormd door Cisco DNA Center. In dat geval: verwijder de WLC uit Inventory, breek de HA, ontdek beide WLC's, en laat Cisco DNA Center de HA vormen.

---

**Opmerking:** deze vereiste kan in latere versies van Cisco DNA Center worden gewijzigd.

---

4.3. Cisco DNA Center heeft het DNAC-CA-trustpoint en -certificaat niet gemaakt.

- Controleer Stap 2 en Stap 3 om dit probleem op te lossen.

4.4. Cisco DNA Center heeft de `sdn-network-infra-iwan` trustpoint en certificaat.

- Controleer Stap 2 en Stap 3 om dit probleem op te lossen.

4.5. Cisco DNA Center heeft niet op de Assurance-configuratie gedrukt.

- Het commando `show network-assurance summary` toont netwerkverzekering als **Disabled**:

```
<#root>
```

```
DC9800-WLC#
```

```
show network-assurance summary
```

```
-----  
Network-Assurance          :  
  
Disabled  
  
Server Url                  :  
ICap Server Port Number    :  
Sensor Backhaul SSID       :  
Authentication              : Unknown
```

- Zorg ervoor dat de WLC Device Controllability heeft ingeschakeld, zoals dit is vereist om Cisco DNA Center de configuratie te kunnen doordrukken. Apparaatbesturing kan worden ingeschakeld tijdens het detectieproces of zodra de WLC op de inventaris staat en wordt beheerd door Cisco DNA Center. Naar het **Inventory** pagina. Kies de **device > Actions > Inventory > Edit Device > Device Controllability > Enable**.

4.6. Cisco DNA Center drukt de configuratie van het telemetrieabonnement niet door.

- Zorg ervoor dat de WLC de abonnementen heeft met de **show telemetry ietf subscription all** uit.
- Als dit niet het geval is, controleer dan Stap 2 en Stap 3 om dit probleem op te lossen.

4.7. De TLS-handdruk tussen de WLC en Cisco DNA Center mislukt omdat het Cisco DNA Center-certificaat niet door de WLC kan worden gevalideerd.

Dit kan te wijten zijn aan vele redenen, de meest voorkomende zijn hier vermeld:

4.7.1. Het certificaat van Cisco DNA Center is verlopen of ingetrokken of bevat niet het IP-adres van Cisco DNA Center in de alternatieve naam van het onderwerp (SAN).

- Zorg ervoor dat het certificaat overeenkomt met de beste praktijken die in de [best practice-gids voor best practices van Cisco DNA Center Security zijn](#) gespecificeerd.

4.7.2. De herroepingscontrole mislukt omdat de certificaatherroepingslijst (CRL) niet kan worden opgehaald.

- Er kunnen vele redenen voor de CRL-herwinning zijn om te falen, zoals een DNS-mislukking, firewallkwestie, connectiviteitskwestie tussen WLC en het CRL Distribution Point (CDP), of één van deze bekende kwesties:
  - Cisco bug-id [CSCvr41793](#) - PKI: voor CRL-ophalen wordt geen HTTP-contentlengte gebruikt.
  - Cisco bug-id [CSCvo03458](#) - PKI "herroepingscontrole crl none" werkt niet als CRL niet bereikbaar is.
  - Cisco bug-id [CSCue73820](#) - PKI debugt niet duidelijk over fout bij parseren van CRL.
- Als tijdelijke oplossing configureren **revocation-check none** in het kader van de DNAC-CA trustpoint.

4.7.3. Certificaatfout "De certificaatketen van de peer is te lang om te worden geverifieerd".

- Controleer de uitvoer van het **show platform software trace message mdt-pubd chassis active R** uit.
- Als dit "Peer certificate chain is too long to be verified" controleer vervolgens:

Cisco bug-id [CSCvw09580](#) - 9800 WLC neemt de diepte van Cisco DNA Center-certificaatketens niet over met 4 & meer.

- Om dit op te lossen, importeert u het certificaat van de tussenliggende CA die het Cisco DNA Center-certificaat heeft afgegeven, in een vertrouwenspunt op de WLC met deze opdracht: **echo | openssl s\_client -connect**

```
:443 -showcerts
```

---

**Opmerking:** hiermee wordt een lijst van certificaten in de vertrouwensketen (PEM-gecodeerd) gegenereerd, zodat elk certificaat begint met -----BEGIN CERTIFICAAT-----. Verwijs naar de URL die in de sectie Workaround wordt vermeld en voer de stappen uit om het DNAC-CA certificaat te configureren, maar voer niet het root-CA certificaat in. Importeer in plaats daarvan het certificaat van de problematische CA.

---

#### 4.7.4. WLC-certificaat verlopen.

- Wanneer de versie van Cisco DNA Center 1.3.3.7 of eerder is, kan het WLC-certificaat zijn verlopen. Wanneer de versie van Cisco DNA Center 1.3.3.8 of hoger is (maar niet 2.1.2.6 of hoger), kan dit nog steeds een probleem zijn als het certificaat vóór de upgrade van versie 1.3.3.7 of eerder is verlopen.
- Controleer de einddatum van de geldigheid in de output van de `show crypto pki certificates sdn-network-infra-  
iwan` uit.

4.8. De service Collector-Joxie op Cisco DNA Center accepteert de verbinding via de WLC niet omdat de inventaris-beheerder niet heeft gemeld dat het nieuwe apparaat geschikt is.

- Voer deze opdracht in op het Cisco DNA Center CLI om de lijst met apparaten te controleren die bekend zijn bij osxe-Collector:

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

- Om alleen de lijst van hostnamen en IP-adressen te krijgen, parse de uitvoer met jq met deze opdracht:

Op Cisco DNA Center 1.3 en hoger:

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

Op Cisco DNA Center 1.3.1 en hoger:

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

- Als deze lijst de WLC niet bevat, start dan de Collector-iosxe service opnieuw en bevestig of dit het probleem oplost.
- Als een herstart van alleen Collector-iosxe niet helpt, kan een herstart van de Collector-Manager service helpen om dit probleem op te lossen.

---

**Tip:** om een service opnieuw te starten, voert u `magctl service restart -d`

- Indien de uitvoer van de opdracht `show telemetry internal connection` nog steeds "Connecting", staart de `collector-iosxe` logbestanden voor de fout:

---

**Tip:** om een logbestand te schaduwen, voert u het veld in `magctl service logs -rf` uit. In dit geval `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)
```

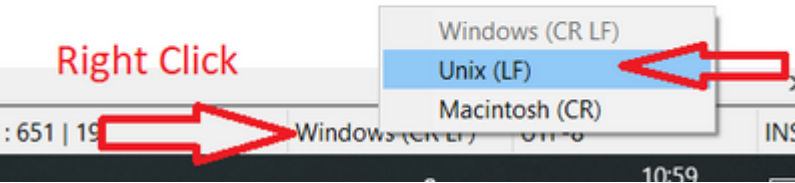
- Als u deze fout ziet, opent u het certificaat dat is toegevoegd aan het Cisco DNA Center, zowel de `.key-` als `.pem-`bestanden (certificaatketen) in Kladblok++. In Kladblok++ navigeren naar **View > Show Symbol > Show All Characters**.
- Als je zoiets hebt:

```

-----BEGIN CERTIFICATE REQUEST-----
MIIDzjCCArYCAQAwQxOzAjBgNVBAYTAkdCMRiWkEAYDVQQIDAlCZXJrc2hpcmUx
EDAOBgNVBAcMBjE1YWRpbmVkbmVhZDc3b3RjY29yZS80MDEwNzI1MjY2ODQx
BgNVBAsMEkNvbnBvcnR0ZSBOZXR3b3RjY29yZS80MDEwNzI1MjY2ODQx
c3R1bXMueHJpdmF0ZSBOZXR3b3RjY29yZS80MDEwNzI1MjY2ODQx
QHZpcmdpbmllZGllLmNvLnVrMlIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
AQEAqZlPszGCafwuoadcIoR+yNIE6j16/7VbzXDF5Ay5Lq9pU9KLFtPfnPV5
8y0b1hIqSf7cXxNZZ10SCRcGrw8M4ZWjClDBY1FNJUfZQJaJSDkL/k/975ud
HrDIPMOBjzyZQxkpy3Rwem9vsr3De6hrYvo2t4wq8vtznPLUr48TQDdy89av
FaVwGyxCsIxqESLR/es/L/LPEBQm8v4ph8yi9F/Yqm2rECLw9QAiWhhyVjDC
kUjfYVwvaoQh0eKcMeLMI726zaTz8woyL2clA037VxLfSuEz51F7hLtP5kx
a9zfhCxU+7Mely4po0VxthoOrQIDAQABoIHDMIHABgkqhkiG9w0BCQ4xgbI
CQYDVROTBAlwADALBgNVHQ8EBAMCBeAwgZQGA1UdEQSBjDCBiYIZY29ycC
LnN5c3R1bXMueHJpdmF0ZSBOZXR3b3RjY29yZS80MDEwNzI1MjY2ODQx
cml2YXR1hwQKSAXLhwQKSAXNhWQKSAXNhwQKSAXOHWQKSX8BhwQKSX8C
hwQKS8EhwQKS8BhwQKS8CchwQKS8DhwQKS8EhwQKS8BhwQKS8CchwQKS8D
AQA0vWQKknwYff5VcnoGtIsoIjYw/kQ438UW7gP2XOXoamxgo/1GApo+bX
MUNXgYWo9Yg02cmDVV8aKqbCUt0QnaEsybJbrXqW33ZBKLLlQjFgSX/Ngte
ZolYHqKrC6vjCfYqRvWs7JAS3WjUknoRfgOAIb7LxPSAdh7df8aoiG6gC
N8FdvjP14zV1vYL11Bvq3TCqN946h7FxtxU4mKcH1VfUqM5eL7hTuOCvj
ZuEHEn0vywgnV/aaGmKpRbRA9gzoXkmCfdiDBhK/aLNCXqoLsXe5zgCUa
nmPzUJEmlYrKdf9nc4TIVFhZ
-----END CERTIFICATE REQUEST-----

```

Ga vervolgens naar:



En bewaar de certificaten.

- Voeg deze nogmaals toe aan het Cisco DNA Center en controleer of de `show telemetry internal connection` de opdracht toont nu "Active".

4.9. Gerelateerde gebreken:

- Cisco bug-id [CSCvs78950](#) - WLC naar Wolverine cluster telemetrieverbinding in 'Connecting' staat.
- Cisco bug-id [CSCvr98535](#) - Cisco DNA Center configureert geen HTTP-broninterface voor PKI - WLC-telemetrieleases 'Connecting'.

Stap 5. Telemetriestatus is actief, maar er zijn nog steeds geen gegevens te zien in Assurance.

Controleer de huidige status van de interne telemetrieverbinding met deze opdracht:

```

</root>
dna-9800#
show telemetry internal connection

Telemetry connection

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

```



Mogelijke defecten:

- Cisco bug-id [CSCvu27838](#) - geen draadloze betrouwbaarheidsgegevens van 9300 met eWLC.
- Cisco bug-id [CSCvu00173](#) - Assurance API-route niet geregistreerd na upgrade naar 1.3.3.4 (niet specifiek voor eWLC).

## Tijdelijke oplossing

Als sommige of alle vereiste configuratie niet in WLC is, probeer dan te bepalen waarom de configuratie niet aanwezig is. Controleer de relevante logbestanden als er een overeenkomst voor een defect is. Daarna, overweeg deze opties als tijdelijke oplossing.

### Cisco DNA Center versie 2.x

Navigeer in de Cisco DNA Center GUI naar de **Inventory** pagina. Kies de **WLC > Actions > Telemetry > Update Telemetry Settings > Force Configuration Push > Next > Apply**. Daarna, wacht een tijdje tot de WLC het resynchronisatieproces beëindigt. Controleer dat Cisco DNA Center de configuratie doordrukt die in het gedeelte Achtergrondinformatie van dit document is vermeld en controleer of de configuratie van de zekerheid op de WLC aanwezig is met de `show network-assurance summary` uit.

### Cisco DNA Center versie 1.x

Dit kan ook voor Cisco DNA Center 2.x worden gebruikt als de vorige GUI-methode nog steeds niet het gewenste effect heeft.

- Het `sdn-network-infra-iwan` trustpoint en/of certificaat wordt gemist.

Neem contact op met het Cisco Technical Assistance Center (TAC) om de Cisco DNA Center Assurance-certificaten en abonnementen handmatig te installeren.

- De configuratie van de netwerkbeveiliging is niet aanwezig.

Zorg ervoor dat het VIP-adres van de onderneming Cisco DNA Center vanuit de WLC kan worden bereikt. Configureer vervolgens de sectie handmatig zoals in het volgende voorbeeld:

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

---

**Opmerking:** op de vijfde regel noteer de ruimte tussen X.X.X.X en /ca/ en ook de ruimte tussen /ca/ en pem.

---

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.