

Resolución de problemas de datos sin garantía en el WLC 9800 en Cisco Catalyst Center

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Resolución de problemas de datos sin garantía de WLC en Catalyst Center](#)

[Solución Alternativa](#)

[Catalyst Center Versión 2.x](#)

[Catalyst Center Versión 1.x](#)

Introducción

Este documento describe cómo resolver problemas cuando Cisco Catalyst Center no muestra ningún dato de Assurance para un controlador de LAN inalámbrica (WLC) Catalyst serie 9800.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:


- Uso de la `maglev` CLI de Catalyst Center
- Base básica de Linux
- Conocimiento de los certificados en Catalyst Center y en la plataforma Catalyst 9800


Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo Catalyst Center de 1ª o 2ª generación con la versión de software 1.x o 2.x con el paquete Assurance
- WLC Catalyst serie 9800


La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

 Nota: Aunque este documento se escribió inicialmente para Catalyst Center 1.x, la mayor parte es válida para Catalyst Center 2.x.

 Nota: El WLC de Catalyst 9800 ya debe ser detectado por el Centro Catalyst y asignado a un sitio, y debe ejecutar una versión compatible de Cisco IOS® XE. Para obtener más detalles sobre la interoperabilidad, consulte la [matriz de compatibilidad de Catalyst Center](#).

Antecedentes

En el momento del proceso de detección, Catalyst Center envía la siguiente configuración al WLC.

 Nota: Este ejemplo proviene de un controlador inalámbrico para la nube Catalyst 9800-CL. Algunos detalles pueden diferir cuando usted utiliza un dispositivo físico de Catalyst 9800 Series; X.X.X.X es la dirección IP virtual (VIP) de la interfaz empresarial de Catalyst Center y Y.Y.Y.Y es la dirección IP de administración 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
```

Resolución de problemas de datos sin garantía de WLC en Catalyst Center

Paso 1. Verifique que el WLC sea accesible y esté administrado en el inventario de Catalyst Center.

Si el WLC no está en estado administrado, usted debe fijar el alcance o el problema de abastecimiento antes de que usted continúe.



Sugerencia: Verifique los registros del administrador de inventario, el administrador de dispositivos spf y el administrador de servicios spf para identificar la falla.

Paso 2. Verifique que Catalyst Center envíe todas las configuraciones necesarias al WLC.

Asegúrese de que la configuración mencionada en la sección Información en Segundo Plano fue empujada al WLC con estos comandos:

```
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
```

Problemas conocidos:

- ID de bug de Cisco [CSCvs62939](#): Cisco DNA Center no envía la configuración de telemetría a los switches 9xxx después de la detección.
- Cisco bug ID [CSCvt83104](#) - eWLC Assurance config push failure if Netconf candidate datastore exists exists in the device.
- Id. de error de Cisco [CSCvt97081](#): el aprovisionamiento del certificado DNAC-CA eWLC falla para el dispositivo detectado por el nombre DNS.

Registros para verificar:

- dna-wireless-service - para el certificado DNAC-CA y la configuración de telemetría.
- network-design-service - para certificado sdn-network-infra-iwan.

Paso 3. Verifique que los certificados necesarios se crean en el WLC.

Asegúrese de que los certificados se crean correctamente en el WLC con estos comandos:

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

Problemas y limitaciones conocidos:

- ID de bug de Cisco [CSCvu03730](#) - eWLC no está monitoreado en Cisco DNA Center porque el certificado sdn-network-infra-iwan no está instalado (la causa raíz es que el certificado del cliente pki-broker ha expirado).
- Cisco bug ID [CSCvr44560](#) - ENH: Añada soporte para certificados CA que venzan después de 2099 para IOS-XE
- Cisco bug ID [CSCw99759](#) - ENH: Añada soporte para la firma de certificado RSA de 8192 bits

Paso 4. Verifique el estado de la conexión de telemetría.

Asegúrese de que la conexión de telemetría esté en el "Active" estado en el WLC con este comando:

```
<#root>
```

```
wlc-01#
```

```
show telemetry internal connection
```

```
Telemetry connection
```

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

Active

O desde Cisco IOS XE Release 17.7 y versiones posteriores:

```
<#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
```

La dirección IP X.X.X.X debe ser la interfaz de Catalyst Center Enterprise. Si Catalyst Center se configura con VIP, éste debe ser el VIP de la interfaz empresarial. Si la dirección IP es correcta y el estado es "Active", vaya al paso siguiente.

Si el estado es "Connecting" entonces la conexión segura del protocolo de transferencia de hipertexto (HTTPS) del WLC al centro de Catalyst no fue establecida con éxito. Puede haber muchas razones diferentes para esto, las más comunes se enumeran a continuación.

4.1. El VIP de Catalyst Center no es accesible desde el WLC o está en "DOWN" estado.

- En un solo nodo con VIP, el VIP se desactiva cuando la interfaz del clúster se desactiva. Verifique que la interfaz del clúster esté conectada.
- Verifique que el WLC tenga conectividad con el Enterprise VIP (ICMP/ping).
- Verifique que el VIP de Catalyst Center Enterprise esté en el "UP" estado, con este comando:
`ip a | grep en.`
- Verifique que Catalyst Center Enterprise VIP esté configurado correctamente con este comando: `etcdctl get /maglev/config/cluster/cluster_network.`

4.2. El WLC está en alta disponibilidad (HA), la garantía no funciona después del failover.

Esto puede ocurrir si el HA no está formado por el Catalyst Center. En ese caso: quite el WLC del inventario, rompa el HA, descubra ambos WLC, y deje que el centro del Catalyst forme el HA.



Nota: Este requisito puede cambiar en versiones posteriores de Catalyst Center.

4.3. Catalyst Center no creó el punto de confianza y el certificado DNAC-CA.

- Verifique el Paso 2. y el Paso 3. para solucionar este problema.

4.4. Catalyst Center no creó el `sdn-network-infra-iwan` punto de confianza ni el certificado.

- Marque los pasos 2 y 3 para solucionar este problema.

4.5. Catalyst Center no envió la configuración Assurance.

- El comando `show network-assurance summary` muestra Network-Assurance como **Disabled**:

```
<#root>
```

```
DC9800-WLC#
```

```
show network-assurance summary
```

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

- Asegúrese de que el WLC tenga habilitada la controlabilidad del dispositivo, ya que esto es necesario para que el centro de Catalyst presione la configuración. La controlabilidad de dispositivos se puede habilitar en el proceso de detección, o una vez que el WLC está en el inventario y administrado por el centro de Catalyst. Vaya a la **Inventory** página. Seleccione **Device > Actions > Inventory > Edit Device > Device Controllability > Enable**.

4.6. Catalyst Center no introduce la configuración de suscripción de telemetría.

- Asegúrese de que el WLC tiene las suscripciones con el `show telemetry ietf subscription all` comando.
- Si no es así, verifique los pasos 2 y 3 para solucionar este problema.

4.7. El intercambio de señales TLS entre el WLC y el Centro Catalyst falla porque el certificado del Centro Catalyst no puede ser validado por el WLC.

Esto podría deberse a muchas razones, las más comunes se enumeran aquí:

4.7.1. El certificado de Catalyst Center ha caducado o ha sido revocado, o bien no dispone de la dirección IP de Catalyst Center en el nombre alternativo del sujeto (SAN).

- Asegúrese de que el certificado coincida con las prácticas recomendadas especificadas en la [Guía de prácticas recomendadas de seguridad de Catalyst Center](#).

4.7.2. La comprobación de revocación falla porque no se puede recuperar la lista de revocación de certificados (CRL).

- Puede haber muchas razones para que la recuperación de CRL falle, como una falla de

DNS, un problema de firewall, un problema de conectividad entre el WLC y el punto de distribución de CRL (CDP), o uno de estos problemas conocidos:

- Cisco bug ID [CSCvr41793](#) - PKI: La recuperación de CRL no utiliza la longitud de contenido HTTP.
- El ID de bug de Cisco [CSCvo03458](#) - PKI "revocation check crl none" no se repliega si la CRL no es accesible.
- ID de bug de Cisco [CSCue73820](#) - Los debugs PKI no son claros sobre el fallo del análisis de CRL.
- Como solución alternativa, configure `revocation-check none` bajo el punto de confianza de DNAC-CA.


4.7.3. Error de certificado "La cadena de certificados de par es demasiado larga para verificarla".

- Verifique el resultado del `show platform software trace message mdt-pubd chassis active R` comando.
- Si se muestra este "Peer certificate chain is too long to be verified" mensaje, compruebe:

El ID de bug de Cisco [CSCvw09580](#) - 9800 WLC no toma la profundidad de las cadenas del certificado del centro de DNA de Cisco con 4 y más.

- Para corregir esto, importe el certificado de la CA intermedia que emitió el certificado del centro Catalyst, en un punto de confianza en el WLC, con este comando: `echo | openssl s_client -connect`

```
:443 -showcerts
```

 Nota: Esto genera una lista de los certificados de la cadena de confianza (codificados PEM), por lo que cada certificado comienza con -----BEGIN CERTIFICATE-----. Consulte la URL mencionada en la sección Solución alternativa y ejecute los pasos para configurar el certificado DNAC-CA, pero no importe el certificado de CA raíz. En su lugar, importe el certificado de la CA problemática.

4.7.4. Certificado WLC caducado.

- Cuando la versión de Catalyst Center es 1.3.3.7 o anterior, el certificado de WLC podría haber caducado. Cuando la versión de Catalyst Center es 1.3.3.8 o posterior (pero no 2.1.2.6 o posterior), esto puede seguir siendo un problema si el certificado expiró antes de la actualización de la versión 1.3.3.7 o anterior.
- Compruebe la fecha de finalización de validez en el resultado del `show crypto pki certificates sdn-network-infra-iwan` comando.

4.8. El servicio colector-iosxe de Catalyst Center no acepta la conexión del WLC porque el servicio de gestión de inventario no le notificó el nuevo dispositivo.

- Para verificar la lista de dispositivos conocidos por iosxe-collector, ingrese este comando en la CLI de Catalyst Center:

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

- Para obtener solamente la lista de hostnames y direcciones IP, analice el resultado con jq con este comando:

En Catalyst Center 1.3 y versiones posteriores:

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

En Catalyst Center 1.3.1 y versiones anteriores:

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

- Si esta lista no contiene el WLC, reinicie el servicio collector-iosxe y confirme si esto resuelve el problema.
- Si un reinicio de collector-iosxe por sí solo no ayuda, un reinicio del servicio de collector-manager puede ayudar a resolver este problema.



Sugerencia: Para reiniciar un servicio, introduzca `magctl service restart -d`

-
- Si el resultado del comando `show telemetry internal connection` sigue siendo "Connecting", busque el error en los collector-iosxe registros:



Sugerencia: Para seguir un archivo de registro, ingrese el `magctl service logs -rf` comando. En este caso, `magctl service logs -rf collector-iosxe | lq..`

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

- Si ve este error, abra el certificado que se agregó al Catalyst Center, tanto sus archivos .key como .pem (cadena de certificados) en Notepad++. En el Bloc de notas++, vaya a `View > Show Symbol > Show All Characters`.
- Si tiene algo como esto:

Paso 5. El estado de telemetría está activo, pero aún así, no se ven datos en Assurance.

Verifique el estado actual de la conexión interna de telemetría con este 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

Posibles defectos:

- ID de bug de Cisco [CSCvu27838](#) - No hay datos de garantía inalámbricos de 9300 con eWLC.
- ID de bug de Cisco [CSCvu00173](#) - La ruta API de la garantía no se registra después de la actualización a 1.3.3.4 (no específica a eWLC).

Solución Alternativa

Si parte o toda la configuración requerida no está en el WLC, intente determinar por qué la configuración no está presente. Verifique los archivos de registro relevantes si hay una coincidencia para un defecto. Después de eso, considere estas opciones como una solución alternativa.

Catalyst Center Versión 2.x

En la GUI de Catalyst Center, navegue hasta la **Inventory** página. Elija el **WLC > Actions > Telemetry > Update Telemetry Settings > Force Configuration Push > Next > Apply**. Después de eso, espere algún tiempo hasta que el WLC termine el proceso de resincronización. Verifique que Catalyst Center presione la configuración mencionada en la sección Información en Segundo Plano de este documento y verifique que la configuración Assurance esté presente en el WLC con el `show network-assurance summary` comando.

Catalyst Center Versión 1.x

Esto también se puede utilizar para Catalyst Center 2.x si el método GUI anterior aún no tiene el efecto deseado.


- Falta el `sdn-network-infra-iwan` punto de confianza o el certificado.

Póngase en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) para instalar manualmente los certificados y suscripciones de Catalyst Center Assurance.

- No hay configuración de garantía de red.

Asegúrese de que la dirección VIP empresarial de Catalyst Center sea accesible desde el WLC. A continuación, configure la sección manualmente como se muestra en el siguiente ejemplo:

```
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
```

 Nota: En la quinta línea, observe el espacio entre X.X.X.X y /ca/ y también el espacio entre /ca/ y pem.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).