

Dépannage de données sans assurance dans le WLC 9800 sur Cisco Catalyst Center

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Dépannage de données sans assurance à partir du WLC sur Catalyst Center](#)

[Solution de contournement](#)

[Catalyst Center Version 2.x](#)

[Catalyst Center version 1.x](#)

Introduction

Ce document décrit comment dépanner lorsque Cisco Catalyst Center n'affiche aucune donnée Assurance pour un contrôleur LAN sans fil (WLC) de la gamme Catalyst 9800.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :


- Utilisation de l'interface de ligne de `maglev` commande Catalyst Center
- Base Linux de base
- Connaissance des certificats sur Catalyst Center et sur la plate-forme Catalyst 9800


Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliance Catalyst Center 1re ou 2e génération avec logiciel version 1.x ou 2.x avec package Assurance
- WLC de la gamme Catalyst 9800


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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

 Remarque : bien que ce document ait été initialement écrit pour Catalyst Center 1.x, la plupart d'entre eux sont valides pour Catalyst Center 2.x.

 Remarque : le WLC Catalyst 9800 doit être déjà détecté par Catalyst Center et attribué à un site, et doit exécuter une version compatible de Cisco IOS® XE. Pour plus de détails sur l'interopérabilité, référez-vous à la [matrice de compatibilité de Catalyst Center](#).

Informations générales

Au moment du processus de détection, Catalyst Center transmet la configuration suivante au WLC.

 Remarque : cet exemple provient d'un contrôleur sans fil cloud Catalyst 9800-CL. Certains détails peuvent varier lorsque vous utilisez un appareil physique de la gamme Catalyst 9800 ; X.X.X.X est l'adresse IP virtuelle (VIP) de l'interface d'entreprise Catalyst Center et Y.Y.Y.Y est l'adresse IP de gestion du 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
```

Dépannage de données sans assurance à partir du WLC sur Catalyst Center

Étape 1. Vérifiez que le WLC est accessible et géré dans l'inventaire Catalyst Center.

Si le WLC n'est pas à l'état Géré, vous devez résoudre le problème d'accessibilité ou de mise en service avant de continuer.



Conseil : vérifiez les journaux Inventory-manager, spf-device-manager et spf-service-manager afin d'identifier la panne.

Étape 2. Vérifiez que Catalyst Center transmet toutes les configurations nécessaires au WLC.

Assurez-vous que la configuration mentionnée dans la section Informations d'arrière-plan a été poussée vers le WLC avec ces commandes :

```
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
```

Problèmes connus :

- ID de bogue Cisco [CSCvs62939](#) - Cisco DNA Center n'envoie pas la configuration de télémétrie aux commutateurs 9xxx après la détection.
- ID de bogue Cisco [CSCvt83104](#) - Échec de la transmission de configuration eWLC Assurance si le datastore candidat Netconf existe sur le périphérique.
- ID de bogue Cisco [CSCvt97081](#) - La mise en service du certificat eWLC DNAC-CA échoue pour le périphérique découvert par le nom DNS.

Journaux à vérifier :

- dna-wireless-service : pour la configuration du certificat et de la télémétrie DNAC-CA.
- network-design-service : pour le certificat sdn-network-infra-iwan.

Étape 3. Vérifiez que les certificats nécessaires sont créés sur le WLC.

Assurez-vous que les certificats sont créés correctement sur le WLC avec ces commandes :

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

Problèmes et limitations connus :

- ID de bogue Cisco [CSCvu03730](#) - eWLC n'est pas surveillé dans Cisco DNA Center parce que le certificat sdn-network-infra-iwan n'est pas installé (la cause principale est que le certificat client pki-broker a expiré).
- ID de bogue Cisco [CSCvr4560](#) - ENH : ajout de la prise en charge des certificats CA expirant après 2099 pour IOS-XE
- ID de bogue Cisco [CSCwc9759](#) - ENH : ajout de la prise en charge de la signature de certificat RSA 8192 bits

Étape 4. Vérifiez l'état de la connexion télémétrique.

Assurez-vous que la connexion de télémétrie est dans l'"Active"état sur le WLC avec cette commande :

```
<#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

Ou à partir de Cisco IOS XE version 17.7 et ultérieure :

```
<#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'adresse IP X.X.X.X doit être l'interface Catalyst Center Enterprise. Si Catalyst Center est configuré avec des VIP, il doit s'agir du VIP de l'interface d'entreprise. Si l'adresse IP est correcte et que l'état est "Active", passez à l'étape suivante.

Si l'état est défini, "Connecting" la connexion HTTPS (Hypertext Transfer Protocol Secure) du WLC à Catalyst Center n'a pas été établie correctement. Il peut y avoir de nombreuses raisons différentes pour cela, les plus courantes sont énumérées ci-dessous.

4.1. Le VIP de Catalyst Center n'est pas accessible depuis le WLC ou est dans l'"DOWN"état.

- Sur un noeud unique avec VIP, le VIP s'arrête lorsque l'interface de cluster s'arrête. Vérifiez que l'interface de cluster est connectée.
- Vérifiez que le WLC est connecté au VIP d'entreprise (ICMP/ping).
- Vérifiez que le VIP de Catalyst Center Enterprise est dans l'"UP"état, avec cette commande :
`ip a | grep en.`
- Vérifiez que le VIP de Catalyst Center Enterprise est correctement configuré avec cette commande : `etcdctl get /maglev/config/cluster/cluster_network.`

4.2. Le WLC est en haute disponibilité (HA), l'assurance ne fonctionne pas après le basculement.

Cela peut se produire si la haute disponibilité n'est pas formée par le Catalyst Center. Dans ce cas : supprimez le WLC de l'inventaire, cassez la HA, découvrez les deux WLC, et laissez Catalyst Center former la HA.



Remarque : cette exigence peut être modifiée dans les versions ultérieures de Catalyst Center.

4.3. Catalyst Center n'a pas créé le point de confiance DNAC-CA et le certificat.

- Pour résoudre ce problème, reportez-vous aux étapes 2 et 3.

4.4. Catalyst Center n'a pas créé le point de confiance `sdn-network-infra-iwan` et le certificat.

- Vérifiez les étapes 2 et 3 pour résoudre ce problème.

4.5. Catalyst Center n'a pas transmis la configuration Assurance.

- La commande affiche `show network-assurance summary` Network-Assurance comme `Disabled`:

```
<#root>
```

```
DC9800-WLC#
```

```
show network-assurance summary
```

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

- Assurez-vous que la fonctionnalité de contrôle des périphériques est activée sur le WLC, car cela est nécessaire pour que Catalyst Center envoie la configuration. La fonctionnalité de contrôle des périphériques peut être activée dans le processus de détection, ou une fois que le WLC est dans l'inventaire et géré par Catalyst Center. Accédez à la `Inventory` page. Sélectionnez `Device > Actions > Inventory > Edit Device > Device Controllability > Enable`.

4.6. Catalyst Center n'applique pas la configuration d'abonnement de télémétrie.

- Assurez-vous que le WLC a les abonnements avec la `show telemetry ietf subscription all` commande.
- Si ce n'est pas le cas, vérifiez les étapes 2 et 3 afin de résoudre ce problème.

4.7. La connexion TLS entre le WLC et Catalyst Center échoue parce que le certificat Catalyst Center ne peut pas être validé par le WLC.

Cela peut être dû à de nombreuses raisons, les plus courantes sont répertoriées ici :

4.7.1. Le certificat Catalyst Center a expiré ou a été révoqué, ou l'adresse IP de Catalyst Center ne figure pas dans le nom alternatif du sujet (SAN).

- Assurez-vous que le certificat correspond aux meilleures pratiques spécifiées dans le [Guide des meilleures pratiques de sécurité de Catalyst Center](#).

4.7.2. La vérification de révocation échoue car la liste de révocation de certificats (CRL) ne peut pas être récupérée.

- Il peut y avoir de nombreuses raisons pour que la récupération de la liste de révocation de certificats échoue, telles qu'une défaillance DNS, un problème de pare-feu, un problème de

connectivité entre le WLC et le point de distribution de la liste de révocation de certificats (CDP), ou un de ces problèmes connus :

- ID de bogue Cisco [CSCvr41793](#) - PKI : la récupération de la liste de révocation de certificats n'utilise pas HTTP Content-Length.
 - ID de bogue Cisco [CSCvo03458](#) - PKI « revocation check crl none » ne se rétablit pas si CRL n'est pas accessible.
 - ID de bogue Cisco [CSCue73820](#) - Les débogages PKI ne sont pas clairs à propos de l'échec d'analyse CRL.
- Pour contourner ce problème, configurez `revocation-check none` sous le point de confiance DNAC-CA.


4.7.3. Erreur de certificat « La chaîne de certificats d'homologue est trop longue pour être vérifiée ».

- Vérifiez le résultat de la `show platform software trace message mdt-pubd chassis active R` commande.
- Si cela s'affiche, "Peer certificate chain is too long to be verified" vérifiez les points suivants :

L'ID de bogue Cisco [CSCvw09580](#) - 9800 WLC ne prend pas en compte la profondeur des chaînes de certificats Cisco DNA Center avec 4 et plus.

- Afin de résoudre ce problème, importez le certificat de l'autorité de certification intermédiaire qui a émis le certificat Catalyst Center, dans un point de confiance sur le WLC, avec cette commande : `echo | openssl s_client -connect`

```
:443 -showcerts
```

 Remarque : ceci produit une liste des certificats dans la chaîne de confiance (codés PEM), de sorte que chaque certificat commence par -----BEGIN CERTIFICATE----- . Référez-vous à l'URL mentionnée dans la section Solution et exécutez les étapes pour configurer le certificat DNAC-CA, mais n'importez pas le certificat CA racine. Importez plutôt le certificat de l'autorité de certification problématique.

4.7.4. Le certificat WLC a expiré.

- Lorsque la version de Catalyst Center est 1.3.3.7 ou antérieure, le certificat WLC peut avoir expiré. Lorsque la version de Catalyst Center est 1.3.3.8 ou ultérieure (mais pas 2.1.2.6 ou ultérieure), cela peut toujours être un problème si le certificat a expiré avant la mise à niveau de la version 1.3.3.7 ou antérieure.
- Vérifiez la date de fin de validité dans le résultat de la `show crypto pki certificates sdn-network-infra-iwan` commande.

4.8. Le service collecteur-isoxe sur Catalyst Center n'accepte pas la connexion du WLC parce qu'il n'a pas été averti du nouveau périphérique par le service gestionnaire d'inventaire.

- Afin de vérifier la liste des périphériques connus par iosxe-collector, entrez cette commande sur la CLI de Catalyst Center :

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

- Afin d'obtenir uniquement la liste des noms d'hôte et des adresses IP, analysez le résultat avec jq avec cette commande :

Sur Catalyst Center 1.3 et versions ultérieures :

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

Sur Catalyst Center 1.3.1 et versions antérieures :

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

- Si cette liste ne contient pas le WLC, redémarrez le service collector-iosxe et vérifiez si cela résout le problème.
- Si un redémarrage de collector-iosxe seul n'aide pas, un redémarrage du service collector-manager peut aider à résoudre ce problème.



Conseil : pour redémarrer un service, saisissez `magctl service restart -d`

-
- Si le résultat de la commande `show telemetry internal connection` est toujours "Connecting", faites suivre les `collector-iosxe` journaux pour l'erreur :



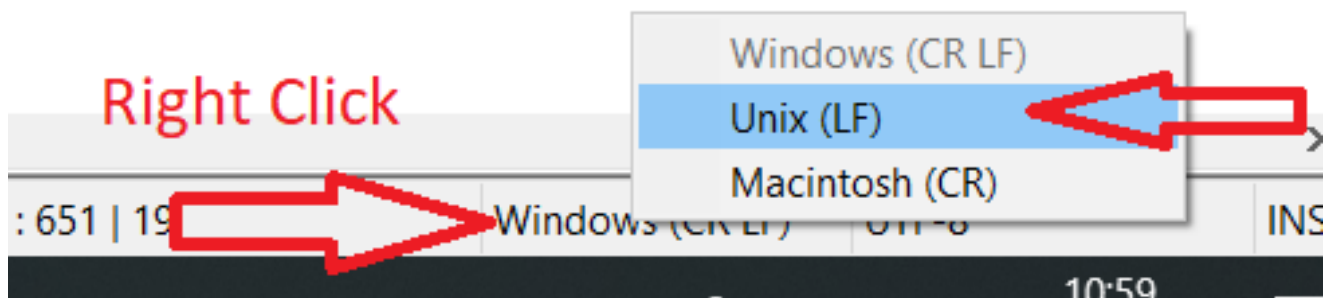
Conseil : pour suivre un fichier journal, entrez la `magctl service logs -rf` commande. Dans ce cas, `magctl service logs -rf collector-iosxe | lq.`

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

- Si vous voyez cette erreur, ouvrez le certificat qui a été ajouté à Catalyst Center, à la fois ses fichiers `.key` et `.pem` (chaîne de certificats) dans le Bloc-notes++. Dans le Bloc-notes++, accédez à `View > Show Symbol > Show All Characters`.
- Si vous avez quelque chose comme ceci :


```
-----BEGIN CERTIFICATE REQUEST-----  
MIIDzjCCArYCAQAwgcQxCzAJBgNVBAYTAkdCMRIwEAYDVQQIDAlCZXJrc2hpcmUx  
EDA0BgNVBAcMB1JlYWRpbmcxGTAXBgNVBAoMEFZpcmdpbmIjbnZWRpYSBMdGQxGzAZ  
BgNVBAsMEkNvcnBvcnF0ZSBOZXR3b3JrczEiMCAGAlUEAwZy29ycC1kbnFjLnN5  
c3RlbXMucHJpdmF0ZTEzMDQEGSgSIB3DQEQJARYkY29ycG9yYXR1Lm5ldHdvcmtz  
QHZpcmdpbm1lZG1hLmNvLnVrMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC  
AQEAqZlPszGCafwuoadcloR+yNIE6jl6/7VbzXDF5Ay5Lq9pU9KLFTpFnPV5jxDK  
8y0blhIqSf7cXxNZzi0SCRcGrw8M4ZWjC1DBY1FNJUfZQJaJSDkL/k/975udSj7p  
HrDipMOBJzyZQxkpy3Rwem9vsr3De6hrYvo2t4wq8vTznPLUr48TQDdy89avkNbb  
FaVwGyxCsIxqE5LR/es/L/LPEBQm8v4ph8yi9F/Yqm2rECLw9QAIWhhyVjDC0Bc/  
kUjfyVvwaQH0eKCMELMi726zaTzS8woyL2clA037VxLfSuEz51F7hLtP5kxuTvFw  
a9zfhCxU+7MelY4po0VxthoOrQIDAQABoIHDMIHABgkqhkiG9w0BCQ4xgbIwga8w  
CQYDVR0TBAlwADALBgNVHQ8EBAMCBeAwgZQGA1UdEQSBjDCBiYIZY29ycC1kbnFj  
LnN5c3RlbXMucHJpdmF0ZiYIY29ycC1kbnFjghlwnBzZXJ2ZXIuc3lzdGVtcy5w  
cm12YXR1hwQKSAXLhwQKSAXMhwQKSAXNhwQKSAXOhwQKS8BhwQKS8ChwQKS8D  
hwQKS8EhwQKS8+BhwQKS8+ChwQKS8+DhwQKS8+EMA0GCSgSIB3DQEQBCwUAA4IB  
AQAvWQKknbwYf5VcnoGTvQIsoIjyW/kQ438UW7gP2XOXoamxgxo/iGApo+bXpCW6  
MUXgYWos9Yg02cmDVV8aKqbCUt0QnaEsybJbrXqW33ZBKL1LqjFgSX/Ngte6TsAm  
ZoLYHqKrC6vjCfYqRVvWs7JA5Y3WjUknoRfg0AIB7LxPSADh7df8aoiG6gCANNQs  
N8FdVJpT4zVivYLilBvq3TCqN946h7FxtxU4mKCh1VfUqM5sL7hTuOCvjqZPQ6mx  
ZuEHEh0vywgnV/aaGmKPbrbRA9gzoXkmCfdiDBhK/aLXCKXqoLsXe5zgCUaYLXTb  
nmPxUJEmlyrKdf9nc4TTVFhZ  
-----END CERTIFICATE REQUEST-----
```

Rendez-vous ensuite sur :



Et enregistrez les certificats.

- Ajoutez-les de nouveau à Catalyst Center et vérifiez si la `show telemetry internal connection` commande affiche maintenant "Active".

4.9. Défauts connexes :

- ID de bogue Cisco [CSCvs78950](#) - Connexion de télémétrie de cluster eWLC à Wolverine à l'état 'Connexion'.
- ID de bogue Cisco [CSCvr98535](#) - Cisco DNA Center ne configure pas l'interface source HTTP pour PKI - la télémétrie eWLC reste « en cours de connexion ».

Étape 5. L'état de télémétrie est actif, mais aucune donnée n'est vue dans Assurance.

Vérifiez l'état actuel de la connexion interne de télémétrie à l'aide de cette commande :

```
<#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
```

Défauts possibles :

- ID de bogue Cisco [CSCvu27838](#) - Aucune donnée d'assurance sans fil de 9300 avec eWLC.
- ID de bogue Cisco [CSCvu00173](#) - Route API d'assurance non enregistrée après la mise à niveau vers 1.3.3.4 (non spécifique à eWLC).

Solution de contournement

Si une partie ou la totalité de la configuration requise ne se trouve pas dans le WLC, essayez de déterminer pourquoi la configuration n'est pas présente. Vérifiez les fichiers journaux appropriés s'il y a une correspondance pour un défaut. Après cela, considérez ces options comme une solution de contournement.

Catalyst Center Version 2.x

Dans l'interface graphique utilisateur de Catalyst Center, accédez à la **Inventory** page. Sélectionnez le **WLC > Actions > Telemetry > Update Telemetry Settings > Force Configuration Push > Next > Apply**. Après cela, attendez un certain temps jusqu'à ce que le WLC termine le processus de resynchronisation. Vérifiez que Catalyst Center applique la configuration mentionnée dans la section Informations d'arrière-plan de ce document et vérifiez que la configuration Assurance est présente sur le WLC avec la `show network-assurance summary` commande.

Catalyst Center version 1.x

Il peut également être utilisé pour Catalyst Center 2.x si la méthode GUI précédente n'a toujours pas l'effet désiré.

- Le `sdn-network-infra-iwan` point de confiance et/ou le certificat est manquant.

Contactez le Centre d'assistance technique Cisco (TAC) pour installer manuellement les certificats et abonnements Catalyst Center Assurance.

- La configuration de l'assurance réseau n'est pas présente.

Assurez-vous que l'adresse IP d'entreprise de Catalyst Center est accessible depuis le WLC. Configurez ensuite la section manuellement comme indiqué dans l'exemple suivant :

```
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
```



Remarque : à la cinquième ligne, notez l'espace entre X.X.X.X et /ca/ ainsi que l'espace entre /ca/ et pem.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.