Dépannage des données sans assurance du WLC 9800 dans Catalyst Center

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Dépannage des données sans assurance du WLC dans Catalyst Center
  - Utilisez l'outil Assurance « Troubleshoot » Machine Reasoning Engine (MRE) dans WLC360
  - Conclusion: Connectivité des périphériques
    - Données et vérification de l'évaluation
    - Éléments à dépanner et à vérifier
    - Connectivité IP
  - Conclusion: Périphérique « non actuellement géré par Catalyst Center »
  - Conclusion: Problèmes de « certificat DNAC-CA (natation) »
  - Conclusion: "Numéro de série du certificat sdn-network-infra-iwan"
- Vérification des données entrantes
- Effectuer une mise à jour télémétrique « forcée »

Introduction

Ce document décrit comment dépanner lorsque Catalyst Center n'affiche aucune donnée Assurance pour un 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 commande Maglev de 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 2e et 3e générations, version 2.3.7.7 et ultérieure

- Contrôleur LAN sans fil (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 écrit à partir de la version 2.3.7.9, cette fonction est également présente dans les versions 3.1.X.

Remarque : Le WLC Catalyst 9800 doit déjà être 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 de l'affectation du site, Catalyst Center transmet la configuration de télémétrie au 9800 au-dessus des configurations SNMP et Syslog.

Remarque : Cet exemple provient d'un contrôleur LAN sans fil en nuage Catalyst 9800-CL. Certains détails peuvent différer 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 des données sans assurance du WLC dans Catalyst Center

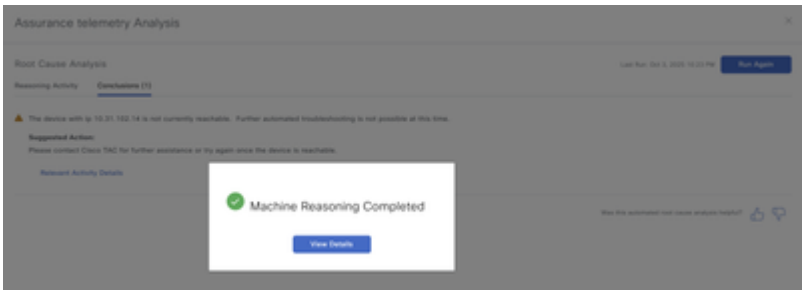
Utilisez l'outil Assurance « Troubleshoot » Machine Reasoning Engine (MRE) dans WLC360

Accédez à la page WLC360. En regard de l'état de santé, l'utilisateur voit le texte bleu « Troubleshoot ».



Cliquez dessus et exécutez le moteur de raisonnement de la machine.

Laissez le moteur de raisonnement s'exécuter jusqu'à son terme.



Consultez l'onglet « Conclusions » pour connaître les problèmes possibles. Si vous recevez une réponse complète sans aucun problème dans la « Conclusion », passez à la section Vérification des données entrantes du présent document.

Si vous ne voyez pas ce lien "Dépannage", alors vous pouvez l'exécuter manuellement sur la page Tools > Network Reasoner dans l'interface graphique utilisateur. Recherchez le workflow "Analyse télémétrique d'assurance".



Conclusion: Connectivité des périphériques

Données et vérification de l'évaluation

Tout d'abord, accédez à la page d'inventaire et assurez-vous que le WLC en question est géré à l'aide de l'adresse IP de gestion sans fil du WLC.

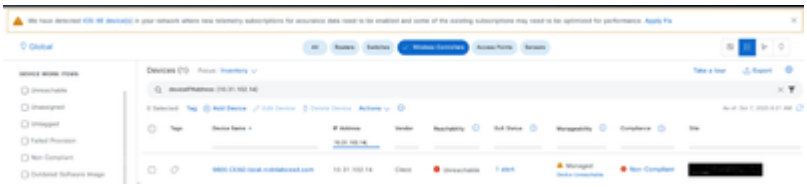
Pour les appliances 9800 : show wireless interface summary



Pour le 9800-CL : show ip interfaces brief | i GigabitEthernet2
Remarque : Cela suppose que l'utilisateur a suivi le guide de déploiement disponible à l'adresse https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/technical-reference/c9800-cl-dg.html#Introduction



Accédez maintenant à la page Inventaire de Catalyst Center.



Cela permet de vérifier qu'il existe des problèmes de connectivité entre Catalyst Center et ce périphérique.

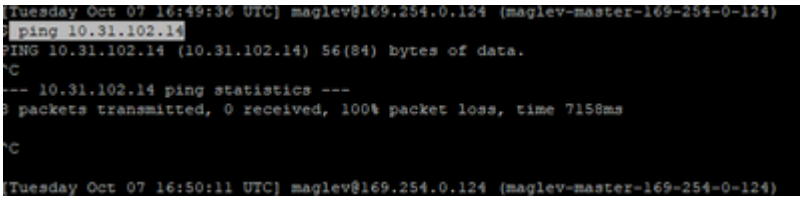
Éléments à dépanner et à vérifier

Connectivité IP

À partir du menu principal, accédez à la page Système > Paramètres. Ensuite, sur la bannière de gauche, allez à la section "Confiance et confidentialité" et sélectionnez "IP Access Control." Une autre méthode consiste à utiliser la recherche globale et la recherche pour "IP Access Control"



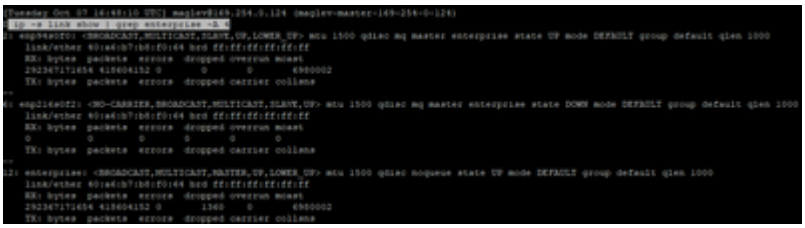
Assurez-vous que les paramètres ici permettent la connectivité au périphérique en question. Ensuite, vérifiez que l'un d'entre eux peut atteindre le périphérique final via ICMP. Pour ce faire, connectez-vous à l'interface de ligne de commande de Catalyst Center et exécutez la commande « ping [IP_Address] » comme indiqué dans ce résultat.



L'élément suivant à examiner est le résultat de la commande "traceroute" de l'interface de ligne de commande de Catalyst Center.



Ensuite, vérifiez qu'il n'y a pas de problèmes de liaison sur Catalyst Center en utilisant la commande "ip -s link show | grep enterprise -A 4"



Si les mesures d'interface semblent acceptables, l'étape suivante consiste à effectuer une capture de paquets (PCAP) des deux côtés de la connexion. Ce guide recommande d'exécuter le premier ensemble de PCAP sur les périphériques en question. Dans cet exemple, les deux périphériques sont un 9800 et le Catalyst Center avec le VIP. Si ce n'est pas possible, exécutez les PCAP le plus près possible des périphériques.

Si des paquets sont envoyés sur le réseau sans passer par l'infrastructure filaire, recherchez sur le réseau filaire des éléments tels que le routage asynchrone, les pare-feu, les NAT et les ACL bloquant les paquets. Une fois ces problèmes résolus, exécutez à nouveau le MRE Assurance « Troubleshoot ».

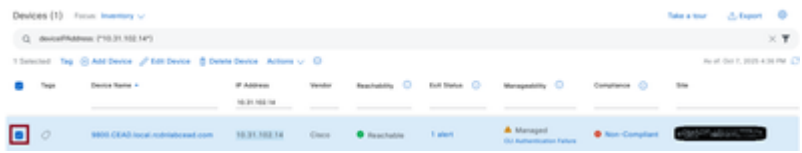
Conclusion: Périphérique « non actuellement géré par Catalyst Center »



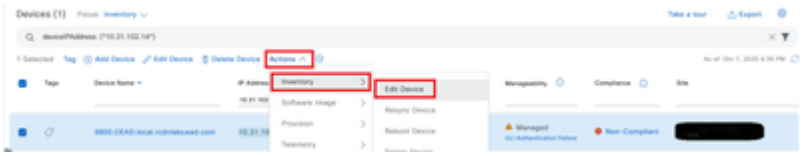
À partir d'aujourd'hui 2.3.7.10, le résultat du workflow peut indiquer de contacter le TAC. Certaines actions peuvent être effectuées avant de contacter le TAC ou de déterminer si un cas de TAC constitue la ligne de conduite immédiate appropriée. Accédez d'abord à la page Inventaire et recherchez le périphérique en question ; Menu principal > Provisionner > Stock. Voici un exemple de mot de passe SSH mal configuré



L'élément suivant à vérifier est que l'état « Accessibilité » n'affiche pas « Inaccessible ». S'il indique « Inaccessible » ou « Inconnu », alors veuillez aller à la section « Connectivité du périphérique ou défaillance des informations d'identification » de ce guide avant d'engager le TAC. S'il affiche « Ping accessible » ou « Accessible », alors on peut passer au dépannage des informations d'identification utilisées par Catalyst Center. Pour ce faire, cochez la case située à gauche du périphérique que vous souhaitez examiner, comme illustré. La case devient bleue avec une coche bleue.

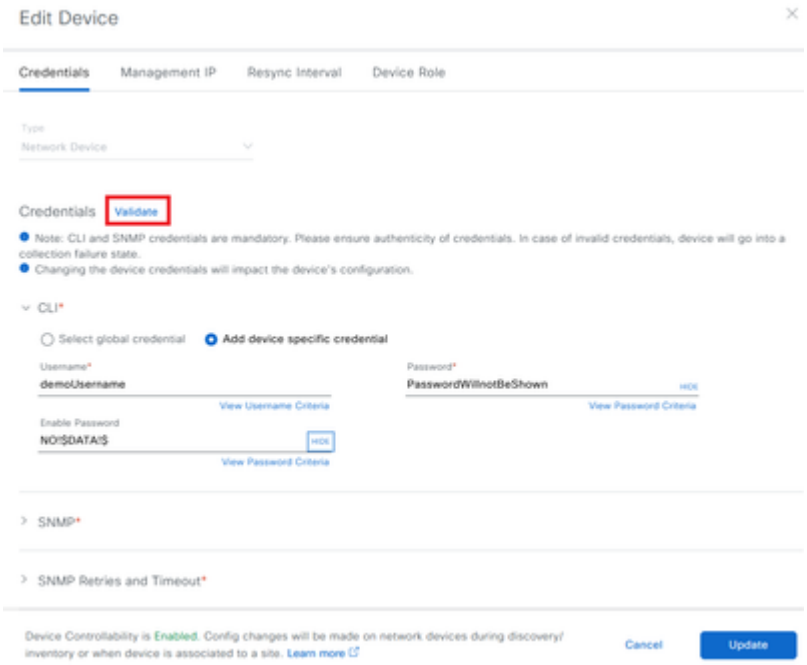


Cliquez ensuite sur "Actions", "Inventaire", et enfin "Modifier le périphérique" comme indiqué :

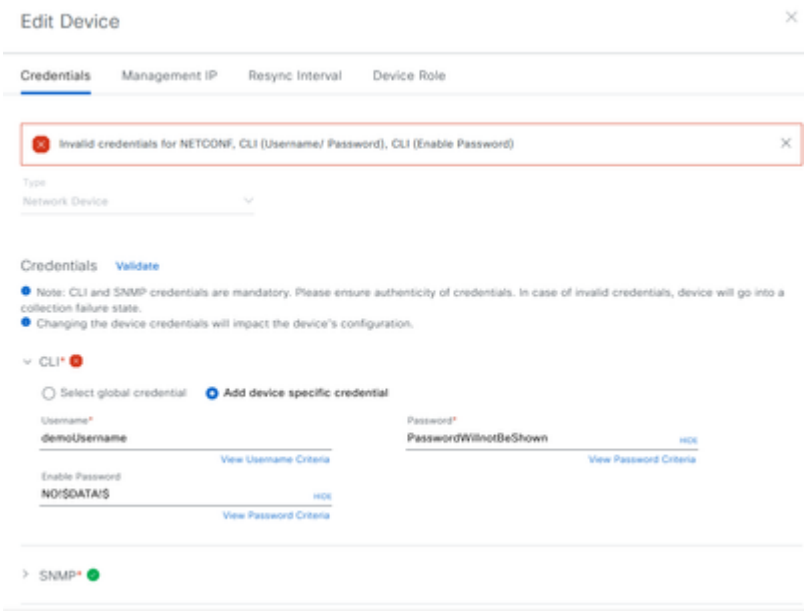


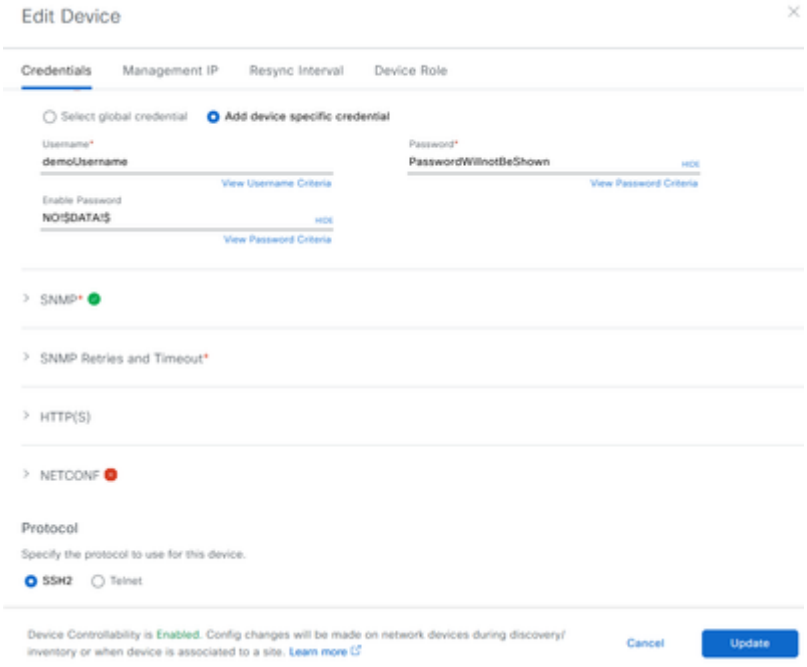
Cette action ouvrira une nouvelle fenêtre qui vous permettra de "Valider" cette configuration. Reportez-vous à cette capture d'écran pour obtenir un exemple.

Remarque : Sur cette page, le "Nom d'utilisateur" sera affiché en texte clair, mais pas les "Mots de passe". À la place, Catalyst Center affiche les mots de passe « NO!$DATA!$ ».



Voici un exemple d'informations d'identification correctes. Reportez-vous au protocole SNMP et aux informations d'identification non valides. Reportez-vous aux sections CLI et Netconf.





Remarque : Les points d'accès sans fil ne seront pas gérés de cette manière. Toutes les données d'AP passent par le WLC.

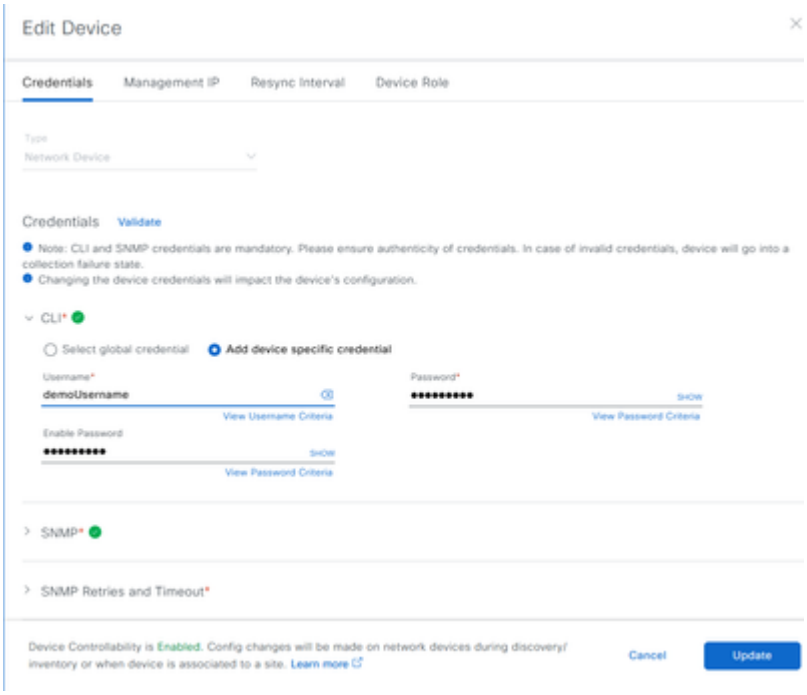
L'accès à l'interface de ligne de commande (SSH) est obligatoire pour tous les périphériques.

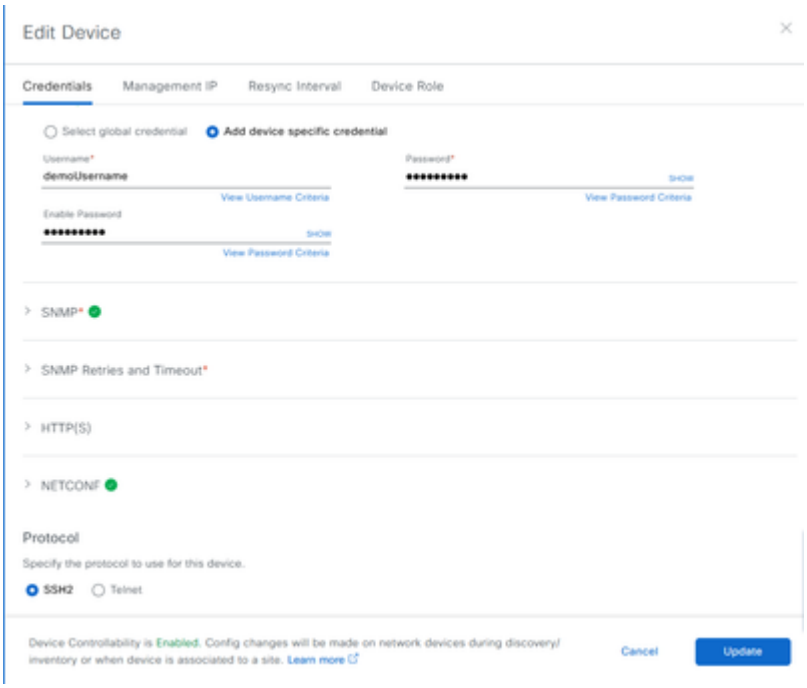
Le protocole SNMP avec un accès en lecture seule minimum est obligatoire pour tous les périphériques.

Netconf est obligatoire pour les WLC 9800 (basés sur Cisco IOS® XE). Netconf fournit une surveillance supplémentaire, par exemple des tableaux de bord PoE pour les commutateurs basés sur Cisco IOS® XE. Il est donc facultatif. Netconf n'est pas utilisé par les périphériques

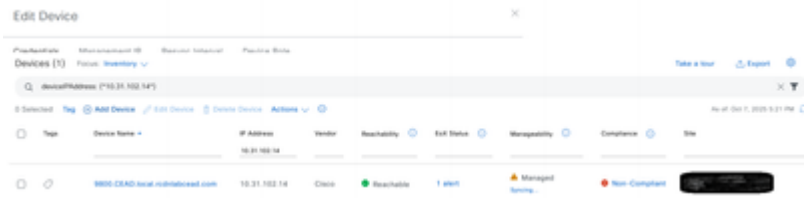
AireOS ou Cisco IOS®.

Après avoir corrigé tous les problèmes et exécuté à nouveau l'option "Valider", on peut voir ceci :





Une fois les erreurs corrigées, cliquez sur le bouton "Update" en bas à gauche. Une fois cette opération effectuée, Catalyst Center met ce périphérique en file d'attente pour une « synchronisation ». Si la file d'attente est vide, la synchronisation démarre immédiatement comme indiqué.



Une fois cette opération effectuée, revenez au résultat de la MRE « Dépannage » pour voir si d'autres éléments doivent être traités. Si rien d'autre ne s'affiche, patientez 15 à 20 minutes pour voir les informations mises à jour. Veuillez contacter le TAC pour obtenir de l'aide si les informations ne sont pas mises à jour après cette date.

Conclusion: Problèmes de « certificat DNAC-CA (natation) »

Voici quelques possibilités qui s'offrent à nous :

- Le certificat concerne un autre Catalyst Center
- La « date/heure actuelle » du périphérique est en dehors de la plage valide
- Le certificat a été remplacé et le périphérique utilise l'ancien certificat.

Veuillez voir lequel des deux est indiqué par le MRE. À partir de là, nous pouvons ensuite passer au 9800 et exécuter quelques commandes pour voir quel problème est à l'origine du problème. Tout d'abord pour déterminer l'heure et la date d'utilisation du périphérique, exécutez la commande show clock.

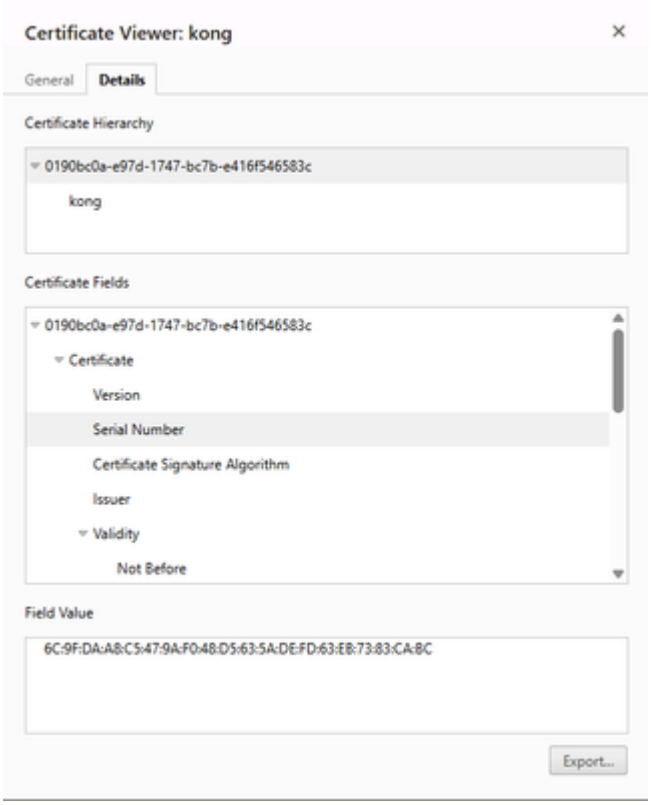
```
9800.CEAD.local#show clock
*02:30:48.038 UTC Thu Oct 9 2025
9800.CEAD.local#
```

Exécutez ensuite show crypto pki certificates DNAC-CA pour extraire les détails du certificat DNAC-CA.

```
9800.CEAD.local#show crypto pki certificates DNAC-CA
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 6C9FDAA8C5479AF048D5635ADEFD63EB7383CABC
  Certificate Usage: General Purpose
  Issuer:
    ou=Cisco DNA Center
    o=Cisco Systems
    cn=0190bc0a-e97d-1747-bc7b-e416f546583c
  Subject:
    ou=Cisco DNA Center
    o=Cisco Systems
    cn=0190bc0a-e97d-1747-bc7b-e416f546583c
  Validity Date:
    start date: 20:45:15 UTC Feb 2 2024
    end   date: 20:45:15 UTC Oct 29 2026
  Associated Trustpoints: DNAC-CA
  Storage: nvram:CiscoDNACent#CABCCA.cer

9800.CEAD.local#
```

Tout d'abord, comparez la « date de début » et la « date de fin » avec la date et l'heure actuelles que le périphérique croit être. Si la Conclusion indique que le certificat ne correspond pas, alors sur le navigateur récupérez les informations du certificat. Le numéro de série doit correspondre. Ceci est un exemple de Chrome d'un numéro de série de certificat correspondant.



Conclusion: "Numéro de série du certificat sdn-network-infra-iwan"



Vérifiez d'abord que la date sur le périphérique est correcte

```
9800.CEAD.local#show clock
*19:41:21.817 UTC Thu Oct 9 2025
9800.CEAD.local#
```

Puis, tirez vers le haut les détails du certificat sdn-network-infra-iwan avec show crypto pki certificates sdn-network-infra-iwan

```
9800.CEAD.local#show crypto pki certificates sdn-network-infra-iwan
Certificate
  Status: Available
  Certificate Serial Number (hex): 676164CD0EED70C9
  Certificate Usage: General Purpose
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    Name: 9800.CEAD.local.rcdnlabcead.com
    cn=C9800-L-C-K9 [redacted] sdn-network-infra-iwan
    hostname=9800.CEAD.local.rcdnlabcead.com
  Validity Date:
    start date: 02:26:47 UTC Oct 4 2025
    end   date: 02:26:47 UTC Oct 4 2026
  Associated Trustpoints: sdn-network-infra-iwan
  Storage: nvram:sdn-network-#70C9.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 6C45E5EC0CB658E1
  Certificate Usage: Signature
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    cn=sdn-network-infra-ca
  Validity Date:
    start date: 23:21:50 UTC Feb 2 2024
    end   date: 23:21:50 UTC Feb 2 2039
  Associated Trustpoints: sdn-network-infra-iwan
  Storage: nvram:sdn-network-#58E1CA.cer
```

Dans ce cas, vérifiez que les dates de validité sont comprises dans les dates que l'appareil croit être.

```
9800.CEAD.local#show crypto pki certificates sdn-network-infra-iwan
Certificate
  Status: Available
  Certificate Serial Number (hex): 676164CD0EED70C9
  Certificate Usage: General Purpose
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    Name: 9800.CEAD.local.rcdnlabcead.com
    cn=C9800-L-C-K9 [redacted] sdn-network-infra-iwan
    hostname=9800.CEAD.local.rcdnlabcead.com
  Validity Date:
    start date: 02:26:47 UTC Oct 4 2025
    end   date: 02:26:47 UTC Oct 4 2026
  Associated Trustpoints: sdn-network-infra-iwan
  Storage: nvram:sdn-network-#70C9.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 6C45E5EC0CB658E1
  Certificate Usage: Signature
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    cn=sdn-network-infra-ca
  Validity Date:
    start date: 23:21:50 UTC Feb 2 2024
    end   date: 23:21:50 UTC Feb 2 2039
  Associated Trustpoints: sdn-network-infra-iwan
  Storage: nvram:sdn-network-#58E1CA.cer
```

Accédez ensuite à Catalyst Center et vérifiez que le numéro de série du certificat correspond.

```
9800.CEAD.local#show crypto pki certificates sdn-network-infra-iwan
Certificate
  Status: Available
  Certificate Serial Number (hex): 676164CD0EED70C9
  Certificate Usage: General Purpose
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    Name: 9800.CEAD.local.rcdnlabcead.com
    cn=C9800-L-C-K9_[redacted] _sdn-network-infra-iwan
    hostname=9800.CEAD.local.rcdnlabcead.com
  Validity Date:
    start date: 02:26:47 UTC Oct 4 2025
    end   date: 02:26:47 UTC Oct 4 2026
  Associated Trustpoints: sdn-network-infra-iwan
  Storage: nvram:sdn-network-#70C9.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 6C45E5EC0CB658E1
  Certificate Usage: Signature
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    cn=sdn-network-infra-ca
  Validity Date:
    start date: 23:21:50 UTC Feb 2 2024
    end   date: 23:21:50 UTC Feb 2 2039
  Associated Trustpoints: sdn-network-infra-iwan
  Storage: nvram:sdn-network-#58E1CA.cer
```

Accédez à la page Menu principal > Système > Paramètres. Sur cette page, recherchez la page « Certificat de périphérique ». Sur cette page, filtrez jusqu'au périphérique en question et vérifiez que le « numéro de série du certificat » correspond.

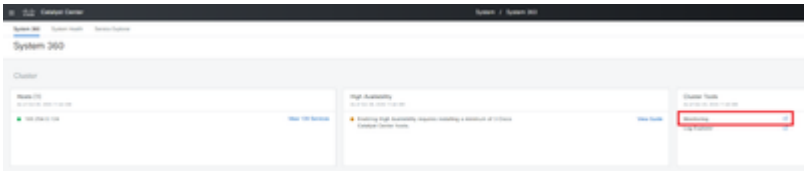


Si cela ne correspond pas, vérifiez que le périphérique est censé se trouver ici et qu'il n'est pas géré par un autre cluster Catalyst Center. Si la défaillance est récente ou si le certificat n'est pas encore arrivé à expiration, contactez le TAC pour une analyse plus approfondie des causes premières si vous le souhaitez. Sinon, allez à la page "Inventaire" et assurez-vous que le périphérique est "Accessible" et "Géré" avec des coches vertes. Si cette page présente un problème, passez à la section Conclusion : Périphérique « non actuellement géré par Catalyst Center » de ce guide et suivez les instructions.

Si tout est vert et entièrement géré, alors veuillez effectuer une mise à jour de télémétrie forcée voir la section Effectuer une mise à jour de télémétrie « forcée ».

Vérification des données entrantes

Accédez à Grafana en accédant à System > System 360 > Monitor. Un nouvel écran s'affichera pour Grafana



Ensuite, accédez au tableau de bord Assurance - Device Processor en cliquant sur la loupe dans la colonne de gauche et en tapant Device Processor

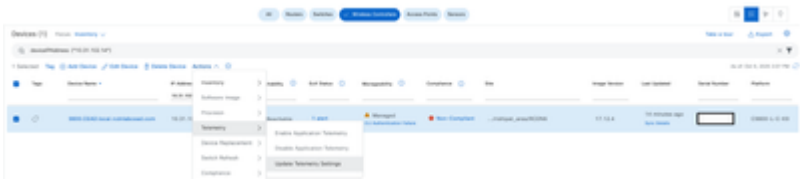


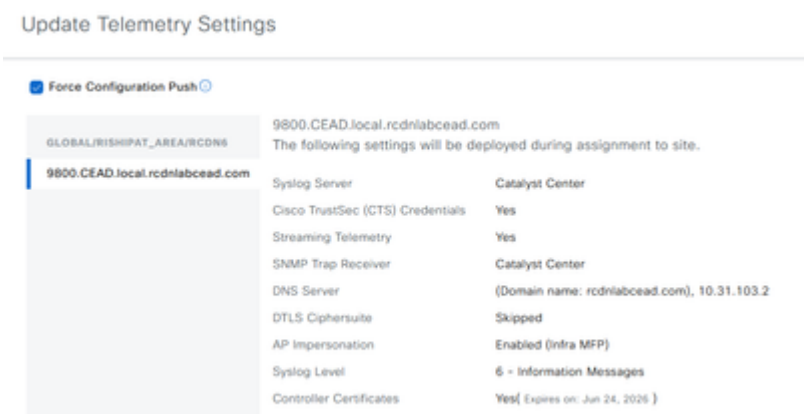
Dans le tableau "Schéma WLC reçu par 5 min" vérifiez le numéro "Mémoire". Ce nombre correspond au nombre de WLC Catalyst 9800 (Cisco IOS® XE) qui envoient du trafic.



Effectuer une mise à jour télémétrique « forcée »

Accédez à Inventory et sélectionnez Update Telemetry Settings comme indiqué.





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.