

Troubleshooting de Dados Sem Garantia no WLC 9800 no Cisco Catalyst Center

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Solucionar problemas de dados sem garantia do WLC no Catalyst Center](#)

[Solução](#)

[Catalyst Center versão 2.x](#)

[Catalyst Center versão 1.x](#)

Introdução

Este documento descreve como solucionar problemas quando o Cisco Catalyst Center não mostra dados de garantia para um Catalyst 9800 Series Wireless LAN Controller (WLC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:


- Uso da CLI do Catalyst Center maglev CLI
- Base básica do Linux
- Conhecimento de certificados no Catalyst Center e na plataforma Catalyst 9800


Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst Center Appliance 1ª ou 2ª geração com software versão 1.x ou 2.x com pacote Assurance
- WLC Catalyst 9800 Series


As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

 Observação: embora este documento tenha sido escrito inicialmente para o Catalyst Center 1.x, a maioria é válida para o Catalyst Center 2.x.

 Observação: a WLC do Catalyst 9800 já deve ser descoberta pelo Catalyst Center e atribuída a um local e deve executar uma versão compatível do Cisco IOS® XE. Para obter mais detalhes sobre interoperabilidade, consulte a [matriz de compatibilidade do Catalyst Center](#).

Informações de Apoio

No momento do processo de descoberta, o Catalyst Center envia a próxima configuração para a WLC.

 Observação: este exemplo é de um Catalyst 9800-CL Cloud Wireless Controller. Alguns detalhes podem ser diferentes quando você usa um dispositivo físico Catalyst 9800 Series; X.X.X.X é o endereço IP virtual (VIP) da interface corporativa do Catalyst Center e Y.Y.Y.Y é o endereço IP de gerenciamento do 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
```

Solucionar problemas de dados sem garantia do WLC no Catalyst Center

Etapa 1. Verifique se a WLC está acessível e gerenciada no inventário do Catalyst Center.

Se a WLC não estiver no status Gerenciado, você deve corrigir o problema de acessibilidade ou provisionamento antes de continuar.

 Dica: verifique os logs do gerenciador de inventário, do gerenciador de dispositivos spf e do gerenciador de serviços spf para identificar a falha.

Etapa 2. Verifique se o Catalyst Center envia todas as configurações necessárias para a WLC.

Certifique-se de que a configuração mencionada na seção Informações de Apoio tenha sido enviada para a WLC com estes 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 conhecidos:

- ID de bug da Cisco [CSCvs62939](#) - O Cisco DNA Center não envia a configuração de telemetria para switches 9xxx após a descoberta.
- ID de bug Cisco [CSCvt83104](#) - Falha no envio de configuração de garantia eWLC se o armazenamento de dados candidato Netconf existir no dispositivo.
- ID de bug Cisco [CSCvt97081](#) - O provisionamento de certificado DNAC-CA do eWLC falha para o dispositivo descoberto pelo nome DNS.

Logs a serem verificados:

- dna-wireless-service - para configuração de telemetria e certificado DNAC-CA.
- network-design-service - para certificado sdn-network-infra-iwan.

Etapa 3. Verifique se os certificados necessários foram criados na WLC.

Certifique-se de que os certificados sejam criados corretamente no WLC com estes comandos:

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

Problemas conhecidos e limitações:

- ID de bug Cisco [CSCvu03730](#) - O eWLC não é monitorado no Cisco DNA Center porque o certificado sdn-network-infra-iwan não está instalado (a causa raiz é que o certificado de cliente pki-broker expirou).
- ID de bug da Cisco [CSCvr44560](#) - ENH: Adicione suporte para certificados CA que expiram após 2099 para IOS-XE
- ID de bug da Cisco [CSCwc99759](#) - ENH: Adicionar suporte para assinatura de certificado RSA de 8.192 bits

Etapa 4. Verifique o status da conexão de telemetria.

Certifique-se de que a conexão de telemetria esteja no "Active" estado na WLC com este comando:

```
<#root>
```

```
wlc-01#
```

```
show telemetry internal connection
```

```
Telemetry connection
```

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

Active

Ou do Cisco IOS XE versão 17.7 e posterior:

```
<#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

O endereço IP do X.X.X.X deve ser a interface do Catalyst Center Enterprise. Se o Catalyst Center estiver configurado com VIPs, ele deverá ser o VIP da interface Enterprise. Se o endereço IP estiver correto e o estado for "Active", vá para a próxima etapa.


Se o estado for "Connecting", a conexão do protocolo HTTPS da WLC com o Catalyst Center não foi estabelecida com êxito. Pode haver muitas razões diferentes para isso, as mais comuns são listadas a seguir.

4.1. O Catalyst Center VIP não pode ser acessado da WLC ou está em "DOWN" status.

- Em um único nó com VIP, o VIP fica inativo quando a interface do cluster fica inativa. Verifique se a interface do cluster está conectada.
- Verifique se a WLC tem conectividade com o Enterprise VIP (ICMP/ping).
- Verifique se o Catalyst Center Enterprise VIP está no "UP" estado, com este comando: `ip a | grep en`.
- Verifique se o Catalyst Center Enterprise VIP está configurado corretamente com este comando: `etcdctl get /maglev/config/cluster/cluster_network`.

4.2. A WLC está em Alta Disponibilidade (HA), a Garantia não funciona após o failover.

Isso pode ocorrer se o HA não for formado pelo Catalyst Center. Nesse caso: remova a WLC do Inventário, quebre o HA, descubra as duas WLCs e deixe o Catalyst Center formar o HA.

 Observação: esse requisito pode ser alterado em versões posteriores do Catalyst Center.

4.3. O Catalyst Center não criou o ponto de confiança e o certificado DNAC-CA.

- Verifique as Etapas 2 e 3 para corrigir esse problema.

4.4. O Catalyst Center não criou o ponto de confiança e o certificado `sdn-network-infra-iwan`.

- Verifique as Etapas 2 e 3 para corrigir esse problema.

4.5. O Catalyst Center não enviou a configuração de Garantia.

- O comando `show network-assurance summary` mostra o 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
```

- Certifique-se de que a WLC tenha a capacidade de controle do dispositivo habilitada, pois isso é necessário para que o Catalyst Center envie a configuração. A capacidade de controle do dispositivo pode ser habilitada no processo de descoberta ou quando a WLC estiver no inventário e for gerenciada pelo Catalyst Center. Navegue até a `Inventory` página. Selecione `Device > Actions > Inventory > Edit Device > Device Controllability > Enable`.

4.6. O Catalyst Center não envia a configuração de assinatura de telemetria.

- Certifique-se de que a WLC tenha as assinaturas com o `show telemetry ietf subscription all` comando.
- Caso contrário, verifique as Etapas 2 e 3 para corrigir esse problema.

4.7. O handshake TLS entre a WLC e o Catalyst Center falha porque o certificado do Catalyst Center não pode ser validado pela WLC.

Isso pode ser devido a muitas razões, as mais comuns estão listadas aqui:

4.7.1. O certificado do Catalyst Center expirou ou foi revogado ou não tem o endereço IP do Catalyst Center no Nome Alternativo do Assunto (SAN).

- Certifique-se de que o certificado corresponda às melhores práticas especificadas no [Guia de Melhores Práticas de Segurança do Catalyst Center](#).

4.7.2. A verificação de revogação falha porque a lista de certificados revogados (LCR) não pode ser recuperada.

- Pode haver muitas razões para a falha da recuperação de CRL, como uma falha de DNS, um problema de firewall, um problema de conectividade entre a WLC e o Ponto de

Distribuição de CRL (CDP - CRL Distribution Point) ou um destes problemas conhecidos:

- ID de bug da Cisco [CSCvr41793](#) - PKI: A recuperação de CRL não usa o comprimento de conteúdo HTTP.
 - ID de bug da Cisco [CSCvo03458](#) - A "verificação de revogação crl none" da PKI não será revertida se a CRL não estiver acessível.
 - ID de bug Cisco [CSCue73820](#) - As depurações de PKI não são claras sobre a falha de análise de CRL.
- Como solução alternativa, configure `revocation-check none` no ponto de confiança DNAC-CA.


4.7.3. Erro de certificado "A cadeia de certificados de pares é demasiado longa para ser verificada".

- Verifique a saída do `show platform software trace message mdt-pubd chassis active R` comando.
- Se isso aparecer, "Peer certificate chain is too long to be verified" marque:

O bug da Cisco ID [CSCvw09580](#) - 9800 WLC não aprofunda as cadeias de certificados do Cisco DNA Center com 4 e mais.

- Para corrigir isso, importe o certificado da CA intermediária que emitiu o certificado do Catalyst Center, para um ponto confiável na WLC, com este comando: `echo | openssl s_client -connect`

```
:443 -showcerts
```

 Observação: isso produz uma lista dos certificados na cadeia de confiança (codificada em PEM), portanto cada certificado começa com -----BEGIN CERTIFICATE----- . Consulte a URL mencionada na seção Solução alternativa e execute as etapas para configurar o certificado DNAC-CA, mas não importe o certificado raiz da CA. Em vez disso, importe o certificado da CA com problemas.

4.7.4. Certificado WLC expirado.

- Quando a versão do Catalyst Center for 1.3.3.7 ou anterior, o certificado WLC pode ter expirado. Quando a versão do Catalyst Center for 1.3.3.8 ou posterior (mas não 2.1.2.6 ou posterior), isso ainda poderá ser um problema se o certificado tiver expirado antes da atualização da versão 1.3.3.7 ou anterior.
- Verifique a data de término da validade na saída do `show crypto pki certificates sdn-network-infra-iwan` comando.

4.8. O serviço coletor-iosxe no Catalyst Center não aceita a conexão da WLC porque não foi notificado do novo dispositivo pelo serviço gerenciador de inventário.

- Para verificar a lista de dispositivos conhecidos pelo iosxe-collector, insira este comando na CLI do Catalyst Center:

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

- Para obter apenas a lista de nomes de host e endereços IP, analise a saída com jq com este comando:

No Catalyst Center 1.3 e posterior:

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

No Catalyst Center 1.3.1 e anterior:

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

- Se essa lista não contiver a WLC, reinicie o serviço collector-iosxe e confirme se isso resolve o problema.
- Se a reinicialização do coletor-iosxe sozinho não ajudar, uma reinicialização do serviço coletor-gerente pode ajudar a resolver esse problema.



Dica: para reiniciar um serviço, insira `magctl service restart -d`

-
- Se a saída do comando ainda `show telemetry internal connection` estiver "Connecting", coloque os collector-iosxe logs finais do erro:



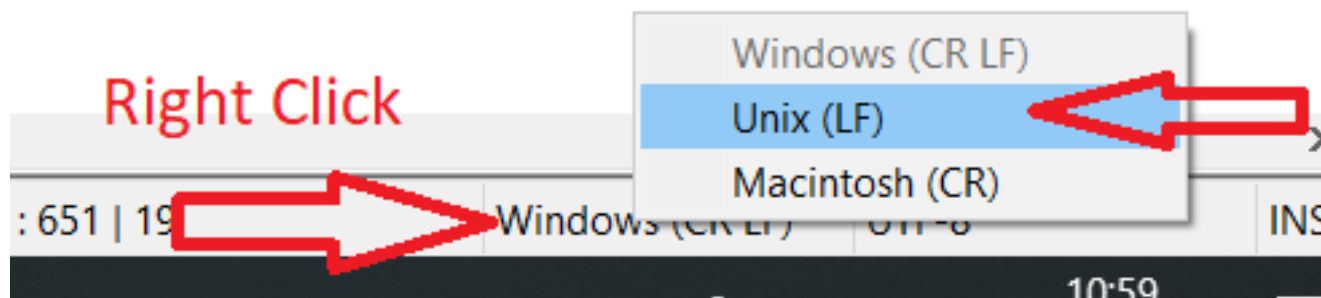
Dica: para finalizar um arquivo de log, insira o `magctl service logs -rf` comando. Neste caso, `magctl service logs -rf collector-iosxe | lq.`

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

- Se você vir esse erro, abra o certificado que foi adicionado ao Catalyst Center, os arquivos `.key` e `.pem` (cadeia de certificados) no Bloco de Notas++. No Notepad++, navegue até `View > Show Symbol > Show All Characters`.
- Se você tiver algo como isto:


```
-----BEGIN CERTIFICATE REQUEST-----  
MIIDzjCCArYCAQAQAwgxCzAJBgNVBAYTAkdCMRIwEAYDVQQIDAlCZXJrc2hpcmUx  
EDA0BgNVBAcMB1JlYWRpbmcxGTAXBgNVBAoMEFZpcmdpbmIjBNZWRpYSBMdGQxGzAZ  
BgNVBAsMEkNvcnBvcnF0ZSBOZXR3b3JrczEiMCAGAlUEAwZy29ycC1kbnFjLnN5  
c3RlbXMucHJpdmF0ZTEzMDEGCSqGSIb3DQEJARYkY29ycG9yYXRlLm5ldHdvcmtz  
QHZpcmdpbm1lZG1hLmNvLnVrMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC  
AQEAqZlPszGCafwuoadcloR+yNIE6jl6/7VbzXDF5Ay5Lq9pU9KLFTpFnPV5jxDK  
8y0blhIqSf7cXxNZzi0SCRcGrw8M4ZWjC1DBY1FNJUfZQJaJSDkL/k/975udSj7p  
HrDipMOBJzyZQxkpy3Rwem9vsr3De6hrYvo2t4wq8vTznPLUr48TQDdy89avkNbb  
FaVwGyxCsIxqE5LR/es/L/LPEBQm8v4ph8yi9F/Yqm2rECLw9QAIWhhyVjDC0Bc/  
kUjfyVvwaQH0eKcMeLMi726zaTZs8woyL2clA037VxLfSuEz51F7hLtP5kxuTvFw  
a9zfhCxU+7MelY4po0VxthoOrQIDAQABoIHDMIHABGkqhkiG9w0BCQ4xgbIwga8w  
CQYDVR0TBAlwADALBgNVHQ8EBAMCBeAwgZQGA1UdEQSBjDCBiYIZY29ycC1kbnFj  
LnN5c3RlbXMucHJpdmF0ZiYIY29ycC1kbnFjghlwbNbzZXJ2ZXIuc3lzdGVtcy5w  
cm12YXRlhwQKSAXLhwQKSAXMhwQKSAXNhwQKSAXOhwQKS8BhwQKS8ChwQKS8D  
hwQKS8EhwQKS8+BhwQKS8+ChwQKS8+DhwQKS8+EMA0GCSqGSIb3DQEBCwUAA4IB  
AQAvWQKknbwYf5VcnoGTvQIsoIjyW/kQ438UW7gP2XOXoamxgxo/iGApo+bXpCW6  
MUXgYWos9Yg02cmDVV8aKqbCUt0QnaEsybJbrXqW33ZBKL1LqjFgSX/Ngte6TsAm  
ZoLYHqKrC6vjCfYqRVvWs7JA5Y3WjUknoRfg0AIB7LxPSADh7df8aoiG6gCNNWQs  
N8FdVJpT4zVivYLilBvq3TCqN946h7FxtxU4mKCh1VfUqM5sL7hTuOCvjq2PQ6mx  
ZuEHEh0vywgnV/aaGmKpbrbRA9gzoXkmCfdiDBhK/aLXCKXqoLsXe5zgCUaYLXTb  
nmPxUJEmlyrKdf9nc4TTVFhZ  
-----END CERTIFICATE REQUEST-----
```

Em seguida, vá para:



E salve os certificados.

- Adicione-os novamente ao Catalyst Center e verifique se o `show telemetry internal connection` comando agora é exibido "Active".

4.9. Defeitos conexos:

- ID de bug Cisco [CSCvs78950](#) - Conexão de telemetria de cluster eWLC para Wolverine no estado 'Conectando'.
- ID de bug Cisco [CSCvr98535](#) - O Cisco DNA Center não configura a interface de origem HTTP para PKI - a telemetria eWLC permanece 'Conectando'.

Etapa 5. O estado de telemetria está ativo, mas ainda assim, nenhum dado é visto na Garantia.

Verifique o status atual da conexão interna de telemetria com 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
```

Possíveis defeitos:

- ID de bug Cisco [CSCvu27838](#) - Sem dados de garantia sem fio do 9300 com eWLC.
- ID de bug Cisco [CSCvu00173](#) - Rota de API de garantia não registrada após a atualização para 1.3.3.4 (não específica para eWLC).

Solução

Se algumas ou todas as configurações necessárias não estiverem na WLC, tente determinar por que a configuração não está presente. Verifique os arquivos de log relevantes se houver uma correspondência para um defeito. Depois disso, considere essas opções como uma solução alternativa.

Catalyst Center versão 2.x

Na GUI do Catalyst Center, navegue até a **Inventory** página. Escolha o **WLC > Actions > Telemetry > Update Telemetry Settings > Force Configuration Push > Next > Apply**. Depois disso, aguarde algum tempo até que o WLC termine o processo de ressincronização. Verifique se o Catalyst Center envia a configuração mencionada na seção **Informações de Fundo** deste documento e verifique se a configuração de Garantia está presente na WLC com o `show network-assurance summary` comando.

Catalyst Center versão 1.x

Isso também pode ser usado para o Catalyst Center 2.x se o método GUI anterior ainda não tiver o efeito desejado.

- O ponto de confiança `sdn-network-infra-iwan` e/ou certificado está ausente.

Entre em contato com o Cisco Technical Assistance Center (TAC) para instalar manualmente os certificados e assinaturas do Catalyst Center Assurance.

- A configuração de garantia de rede não está presente.

Certifique-se de que o endereço VIP corporativo do Catalyst Center possa ser acessado da WLC. Em seguida, configure a seção manualmente, conforme mostrado no próximo exemplo:

```
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
```



Observação: na quinta linha, observe o espaço entre X.X.X.X e /ca/ e também o espaço entre /ca/ e pem.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.