

排除Cisco Catalyst Center上WLC 9800中的无保证数据故障

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[排除来自Catalyst Center上的WLC的无保证数据故障](#)

[解决方法](#)

[Catalyst Center版本2.x](#)

[Catalyst Center版本1.x](#)

简介

本文档介绍当Cisco Catalyst Center未显示Catalyst 9800系列无线局域网控制器(WLC)的任何保证数据时如何进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- Catalyst Center CLI的使^{maglev}用
- 基本Linux基础
- Catalyst Center和Catalyst 9800平台上的证书知识


使用的组件

本文档中的信息基于以下软件和硬件版本：

- Catalyst Center设备第1代或第2代，软件版本为1.x或2.x，带有保证软件包
- Catalyst 9800系列WLC

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

 注：虽然本文档最初是针对Catalyst Center 1.x编写的，但其中大部分内容适用于Catalyst Center 2.x。

 注意：Catalyst 9800 WLC必须已由Catalyst Center发现并分配到站点，且必须运行兼容的Cisco IOS® XE版本。有关互操作性的详细信息，请参阅[Catalyst Center兼容性列表](#)。

背景信息

在发现过程中，Catalyst Center将下一配置推送到WLC。

 注：此示例来自Catalyst 9800-CL云无线控制器。使用物理Catalyst 9800系列设备时，某些详细信息可能会有所不同；X.X.X.X是Catalyst Center企业接口的虚拟IP(VIP)地址，而Y.Y.Y.Y是WLC的管理IP地址。

<#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
```

排除Catalyst Center上WLC中的无保证数据故障

步骤1:验证WLC在Catalyst Center资产中是否可以访问和管理。

如果WLC未处于“托管”状态，则必须在继续之前修复可接通性或调配问题。



提示：检查资产管理器、spf-device-manager和spf-service-manager日志以确定故障。

第二步：验证Catalyst Center是否将所有必要的配置推送到WLC。

确保Background Information（后台信息）部分中提到的配置已使用以下命令推送到WLC：

```
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
```

已知问题：

- 思科漏洞ID [CSCvs62939](#) — 思科DNA中心在发现后不会将遥测配置推送到9xxx交换机。
- Cisco Bug ID [CSCvt83104](#) - eWLC Assurance config push failure if Netconf candidate datastore exists on the device. (如果设备上存在Netconf candidate datastore，则eWLC保障配置推送失败。)
- Cisco Bug ID [CSCvt97081](#) - eWLC DNAC-CA证书调配对于通过DNS名称发现的设备失败。

要验证的日志：

- dna-wireless-service — 用于DNAC-CA证书和遥测配置。
- network-design-service — 用于sdn-network-infra-iwan证书。

第三步：验证已在WLC上创建必要的证书。

确保使用以下命令在WLC上正确创建证书：

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

已知问题和限制：

- Cisco bug ID [CSCvu03730](#) - eWLC在Cisco DNA Center中不受监控，因为未安装sdn-network-infra-iwan证书（根本原因是pki-broker客户端证书已过期）。
- Cisco Bug ID [CSCvr44560](#) - ENH：为IOS-XE添加对2099年后到期的CA证书的支持
- 思科漏洞ID [CSCwc99759](#) — 增强版：添加对8192位RSA证书签名的支持

第四步：验证遥测连接状态。

使用以下命令确保遥测"Active"连接处于WLC上的状态：

```
<#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

或者，从Cisco IOS XE版本17.7及更高版本：

```
<#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

X.X.X.X IP地址必须是Catalyst Center Enterprise接口。如果为Catalyst Center配置了VIP，则这必须是企业接口的VIP。如果IP地址正确且状态为"Active"正确，请继续下一步。


如果状态为"Connecting"则无法成功建立从WLC到Catalyst Center的超文本传输协议安全(HTTPS)连接。导致此问题的原因可能有很多种，下面列出了最常见的原因。

4.1.无法从WLC访问Catalyst Center VIP或处于状"DOWN"态。

- 在带有VIP的单个节点上，当集群接口关闭时，VIP会关闭。检验集群接口是否已连接。
- 检验WLC是否连接到企业VIP(ICMP/ping)。
- 使用以下命令验证Catalyst Center Enterprise "UP"VIP是否处于状态：`ip a | grep eno`。
- 使用以下命令验证是否已正确配置Catalyst Center Enterprise `etcdctl get /maglev/config/cluster/cluster_networkVIP`。

4.2. WLC处于高可用性(HA)状态，故障转移后，保证无法工作。

如果HA不是由Catalyst Center形成的，则会发生这种情况。在这种情况下：从库存中删除WLC，中断HA，发现两个WLC，并让Catalyst Center形成HA。

 注意：此要求可在更高的Catalyst Center版本中更改。

4.3. Catalyst Center未创建DNAC-CA信任点和证书。

- 请检查步骤2.和步骤3.解决此问题。

4.4. Catalyst Center未创建信任点sdn-network-infra-iwan和证书。

- 检查步骤2.和步骤3以解决此问题。

4.5. Catalyst Center未推送保证配置。

- 命令显示`show network-assurance summary`示Network-Assurance为Disabled:

```
<#root>
```

```
DC9800-WLC#
```

```
show network-assurance summary
```

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

- 确保WLC已启用设备可控性，因为Catalyst Center推送配置需要此功能。设备可控性可以在发现过程中启用，或者在WLC位于资产上并由Catalyst Center管理后启用。导航到页Inventory面。选择.Device > Actions > Inventory > Edit Device > Device Controllability > Enable

4.6. Catalyst Center不推送遥测订用配置。

- 确保WLC具有使用该命令的订 show telemetry ietf subscription all用。
- 否则，请检查步骤2和步骤3以解决此问题。

4.7. WLC和Catalyst Center之间的TLS握手失败，因为WLC无法验证Catalyst Center证书。

这可能是由于多种原因，下面列出了最常见的原因：

4.7.1. Catalyst Center证书已过期或已撤销，或者主题备用名称(SAN)中没有Catalyst Center IP地址。

- 确保证书与[Catalyst Center安全最佳实践指南](#)中指定的最佳实践相匹配。

4.7.2.撤销检查失败，因为无法检索证书撤销列表(CRL)。

- CRL检索失败的原因可能很多，例如DNS故障、防火墙问题、WLC和CRL分发点(CDP)之间的连接问题或以下已知问题之一：
 - Cisco Bug ID [CSCvr41793](#) - PKI:CRL检索不使用HTTP Content-Length。
 - Cisco Bug ID [CSCvo03458](#) - PKI“revocation check crl none”在无法访问CRL时不会回退。
 - Cisco Bug ID [CSCue73820](#) - PKI调试不了解CRL解析故障。
- 解决方法：在revocation-check noneDNAC-CA信任点下配置。

4.7.3.证书错误“对等证书链过长，无法验证”。


- 检查命令的输 show platform software trace message mdt-pubd chassis active R出。
- 如果显示此信息“Peer certificate chain is too long to be verified”，请检查：

Cisco Bug ID [CSCvw09580](#) - 9800 WLC不采用Cisco DNA Center证书链深度为4或更多。

- 要解决此问题，请使用以下命令将颁发Catalyst Center证书的中间CA的证书导入到WLC上的信任点echo | openssl s_client -connect

```
:443 -showcerts
```

```
∴。
```

 注：这将生成信任链（PEM编码）中的证书列表，因此每个证书以-----BEGIN CERTIFICATE-----开头。请参阅“解决方法”部分中提到的URL，并执行配置DNAC-CA证书的步骤，但不导入根CA证书。相反，请导入有问题的CA的证书。

4.7.4. WLC证书已过期。

- 当Catalyst Center版本为1.3.3.7或更低版本时，WLC证书可能已过期。当Catalyst Center的版本为1.3.3.8或更高版本（但不是2.1.2.6或更高版本）时，如果证书在从版本1.3.3.7或更早期

本升级之前过期，则仍有可能出现此问题。

- 检查命令输出中的有效结束日 `show crypto pki certificates sdn-network-infra-iwan` 期。

4.8. Catalyst Center 上的收集器 iosxe 服务不接受来自 WLC 的连接，因为库存管理器服务未通知它新设备。

- 要检查 iosxe-collector 已知的设备列表，请在 Catalyst Center CLI 上输入以下命令：

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

- 为了只获取主机名和 IP 地址列表，请使用以下命令使用 jq 解析输出：

在 Catalyst Center 1.3 及更高版本上：

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

在 Catalyst Center 1.3.1 及更低版本上：

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

- 如果此列表不包含 WLC，请重新启动收集器 iosxe 服务，并确认这是否解决了问题。
- 如果单纯重新启动收集器 iosxe 没有帮助，重新启动收集器 — 管理器服务可以帮助解决此问题。



提示：要重新启动服务，请输入 `magctl service restart -d`。

- 如果命令输出仍然 `show telemetry internal connection` 存在，“Connecting”请跟踪日志 `collector-iosxe` 以了解错误：



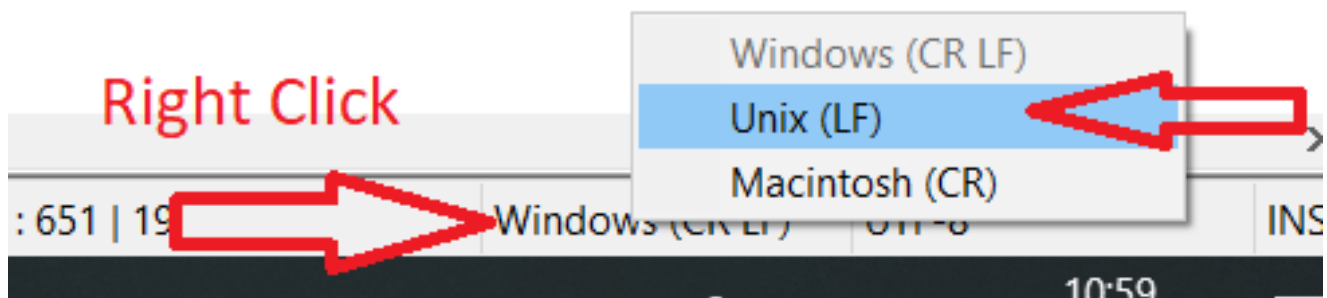
提示：要跟踪日志文件，请输入命令 `magctl service logs -rf`。在本例中，`magctl service logs -rf collector-iosxe | lql`。

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

- 如果看到此错误，请在记事本++中打开已添加到 Catalyst Center 的 .key 和 .pem (证书链) 文件的证书。在记事本++中，导航到 View > Show Symbol > Show All Characters 中。
- 如果您有如下内容：

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIDzjCCArYCAQAQAwgcQxCzAJBgNVBAYTAkdCMRIwEAYDVQQIDAlCZXJrc2hpcmUx  
EDA0BgNVBAcMB1JlYWVpbmVzGTAxBGNVBAoMEFZpcmdpbmVzY29ycC1kbmFjLnN5  
BgNVBAsMEkNvcnBvcnF0ZSBOZXR3b3JrczEiMCAGAlUEAwWZY29ycC1kbmFjLnN5  
c3RlbXMucHJpdmF0ZTEzMDEGCSqGSIb3DQEJARYkY29ycG9yYXR1Lm5ldHdvcmUz  
QHZpcmdpbmVzLzZGlhLmNvLnVrMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC  
AQEAQz1PszGCafwuoadcloR+yNIE6jl6/7VbzXDF5Ay5Lq9pU9KLFTpFnPV5jxDK  
8y0blhIqSf7cXxNZZi0SCRcGrw8M4ZWjC1DBY1FNJUfZQJaJSDkL/k/975udS77p  
HrDipMOBJzyZQxkpy3Rwem9vsr3De6hrYvo2t4wq8vTznPLUr48TQDdy89avkNbb  
FaVwGyxCsIxqE5LR/es/L/LPEBQm8v4ph8yi9F/Yqm2rECLw9QAiWhhyVjDC0Bc/  
kUjfYVvwaQH0eKCMELMi726zaTzS8woyL2clA037VxLfSuEz51F7hLtP5kxuTvFw  
a9zfhCxU+7MelY4po0VxthoOrQIDAQABoIHDMIHABGkqhkiG9w0BCQ4xgbIwga8w  
CQYDVR0TBAlwADALBgNVHQ8EBAMCBeAwgZQGA1UdEQSBjDCBiYIZY29ycC1kbmFj  
LnN5c3RlbXMucHJpdmF0ZlYlY29ycC1kbmFjghlwbNbzZXJ2ZXIuc3lzdGVtcy5w  
cm12YXR1hwQKSAXLhwQKSAXMhwQKSAXNhwQKSAXOhwQKS8BhwQKS8ChwQKS8D  
hwQKS8EhwQKS8+BhwQKS8+ChwQKS8+DhwQKS8+EMA0GCSqGSIb3DQEBCwUAA4IB  
AQAvWQKknbwYf5VcnoGTvQIsoIjyW/kQ438UW7gP2XOXoamxgx0/iGApo+bXpCW6  
MUXgYWos9Yg02cmDVV8aKqbCUt0QnaEsybJbrXqW33ZBKl1LqjFgSX/Ngte6TsAm  
ZoLYHqKrc6vjCfYqRVvWs7JA5Y3WjUknoRfg0AIB7LxPSADh7df8aoiG6gCNNWQs  
N8FdVJpT4zVivYLilBvq3TCqN946h7FxtxU4mKCh1VfUqM5sL7hTuOCvjq2PQ6mx  
ZuEHEh0vywgnV/aaGmKPbrbRA9gzoXkmCfdiDBhK/aLXCKXqoLsXe5zgCUaYLXTb  
nmPxUJEmlyrKdf9nc4TTVfhZ  
-----END CERTIFICATE REQUEST-----
```

然后转至：



并保存证书。

- 再次将其添加到Catalyst Center，并检查命令现在是show telemetry internal connection否显示出"Active"来。

4.9.相关缺陷：

- Cisco Bug ID [CSCvs78950](#) - eWLC到Wolverine群集遥测连接处于“连接”状态。
- 思科漏洞ID [CSCvr98535](#) - Cisco DNA Center不为PKI配置HTTP源接口 — eWLC遥测保持“Connecting”（连接）。

第五步：遥测状态处于活动状态，但在保证中仍然看不到任何数据。

使用以下命令验证遥测内部连接的当前状态：

```
<#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
```

可能的缺陷：

- 思科漏洞ID [CSCvu27838](#) — 没有来自9300的带eWLC的无线保证数据。
- 思科漏洞ID [CSCvu00173](#) — 升级到1.3.3.4后未注册保证API路由（不特定于eWLC）。

解决方法

如果所需的部分或全部配置不在WLC中，请尝试确定配置不存在的原因。如果存在缺陷的匹配项，请检查相关日志文件。然后，将这些选项视为一种解决方法。

Catalyst Center版本2.x

在Catalyst Center GUI上，导航至该Inventory页面。选择WLC > Actions > Telemetry > Update Telemetry Settings > Force Configuration Push > Next > Apply。然后，等待一段时间，直到WLC完成重新同步过程。使用命令验证Catalyst Center是否推送了本文档背景信息部分中提到的配置，并验证WLC上是否存在保证配置。
`show network-assurance summary`置。

Catalyst Center版本1.x

如果之前的GUI方法仍然没有达到预期效果，也可以将此功能用于Catalyst Center 2.x。


- 信任sdn-network-infra-iwan点和/或证书丢失。

请联系思科技术支持中心(TAC)，以手动安装Catalyst Center保证证书和订用。

- 网络保证配置不存在。

确保可以从WLC访问Catalyst Center企业VIP地址。然后手动配置该部分，如下例所示：

```
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
```

 注：在第五行中，注意X.X.X.X和/ca/之间的空格以及/ca/和pem之间的空格。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。