

# Cisco Catalyst Center上のWLC 9800でのNo Assuranceデータのトラブルシューティング

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[Catalyst CenterのWLCからのNo Assuranceデータのトラブルシューティング](#)

[回避策](#)

[Catalyst Centerバージョン2.x](#)

[Catalyst Centerバージョン1.x](#)

---

## はじめに

このドキュメントでは、Cisco Catalyst Center(CatOS)でCatalyst 9800シリーズワイヤレスLANコントローラ(WLC)の保証データが表示されない場合のトラブルシューティング方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Catalyst Center `maglev` CLIの使用
- 基本的なLinux基盤
- Catalyst CenterおよびCatalyst 9800プラットフォームの証明書に関する知識

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Catalyst Centerアプライアンス第1世代または第2世代とソフトウェアバージョン1.xまたは2.xおよびAssuranceパッケージ
- Catalyst 9800シリーズWLC

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

---

 注：このドキュメントは最初はCatalyst Center 1.x用に作成されましたが、そのほとんどはCatalyst Center 2.xにも適用できます。

---

 注:Catalyst 9800 WLCは、Catalyst Centerによってすでに検出され、サイトに割り当てられている必要があります。また、互換性のあるCisco IOS® XEバージョンが稼働している必要があります。相互運用性の詳細については、『[Catalyst Center互換性マトリクス](#)』を参照してください。

---

## 背景説明

ディスカバリプロセスの時点で、Catalyst Centerは次の設定をWLCにプッシュします。

---

 注：この例は、Catalyst 9800-CL Cloud Wireless Controllerのもので、物理Catalyst 9800シリーズアプライアンスを使用する場合は、一部の詳細が異なる場合があります。X.X.X.XはCatalyst Centerエンタープライズインターフェイスの仮想IP(VIP)アドレスで、Y.Y.Y.YはWLCの管理IPアドレスです。

---

```
<#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
```

## Catalyst CenterのWLCからのNo Assuranceデータのトラブルシューティング

ステップ 1 : Catalyst CenterインベントリでWLCが到達可能で管理されていることを確認します。

WLCが管理対象ステータスでない場合は、到達可能性またはプロビジョニングの問題を修正してから続行する必要があります。

---

 ヒント:inventory-manger、spf-device-manager、spf-service-managerのログを確認して、障害を特定します。

---

ステップ 2 : Catalyst Centerが必要なすべての設定をWLCにプッシュすることを確認します。

「背景説明」セクションで説明した設定が、次のコマンドを使用してWLCにプッシュされたことを確認します。

```
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
```

#### 既知の問題：

- Cisco Bug ID [CSCvs62939](#):Cisco DNA Centerが検出後にテレメトリ設定を9xxxスイッチにプッシュしない
- Cisco Bug ID [CSCvt83104](#):eWLC Assurance config push failure if Netconf candidate datastore exists on the device.
- Cisco Bug ID [CSCvt97081](#):DNS名で検出されたデバイスのeWLC DNAC-CA証明書プロビジョニングが失敗する。

#### 確認するログ：

- dna-wireless-service:DNAC-CA証明書およびテレメトリ設定の場合。
- network-design-service:sdn-network-infra-iwan証明書用。

ステップ 3：必要な証明書がWLCで作成されることを確認します。

次のコマンドを使用して、証明書がWLCで正しく作成されたことを確認します。

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

#### 既知の問題と制限事項：

- Cisco Bug ID [CSCvu03730](#):sdn-network-infra-iwan証明書がインストールされていないため（根本的な原因はpki-brokerクライアント証明書の有効期限が切れていることにあります）、eWLCはCisco DNA Centerでモニタされません。
- Cisco Bug ID [CSCvr44560](#) - ENH:IOS-XEに対して2099年以降に期限が切れるCA証明書のサポートを追加
- Cisco Bug ID [CSCwc99759](#):ENH:8192ビットRSA証明書シグニチャのサポートの追加

ステップ 4：テレメトリ接続のステータスを確認します。

次のコマンドを使用して、テレメトリ接続がWLC上の"Active"状態であることを確認します。

```
<#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
```

またはCisco IOS XEリリース17.7以降：

```
<#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
```

X.X.X.XのIPアドレスは、Catalyst Center Enterpriseインターフェイスである必要があります。Catalyst CenterがVIPで設定されている場合、これはエンタープライズインターフェイスのVIPである必要があります。IPアドレスが正しく、状態が正しい場合は、次のステータス"Active"に進みます。

この状態が発生する"Connecting"の場合は、WLCからCatalyst CenterへのHypertext Transfer Protocol Secure(HTTPS)接続が正常に確立されていません。これにはさまざまな理由がある可能性があり、最も一般的なものは次にリストされています。

#### 4.1. Catalyst Center VIPがWLCから到達不能であるか、ステータス"DOWN"である。

- VIPを備えた単一ノードでは、クラスターインターフェイスがダウンするとVIPがダウンします。クラスターインターフェイスが接続されていることを確認します。
- WLCがエンタープライズVIP(ICMP/ping)に接続できることを確認します。
- 次のコマンドを使用して、Catalyst Center Enterprise VIPが"UP"状態であることを確認します。 `ip a | grep en.`
- Catalyst Center Enterprise VIPが次のコマンドで正しく設定されていることを確認します。  
`etcdctl get /maglev/config/cluster/cluster_network.`

#### 4.2. WLCがハイアベイラビリティ(HA)で稼働していて、フェールオーバー後にAssuranceが機能しない。

これは、HAがCatalyst Centerによって形成されていない場合に発生する可能性があります。その場合は、インベントリからWLCを削除し、HAを解除して両方のWLCを検出し、Catalyst CenterでHAを形成します。

 注：この要件は、最近のCatalyst Centerバージョンで変更される可能性があります。

#### 4.3. Catalyst Centerは、DNAC-CAトラストポイントと証明書を作成しませんでした。

- この問題を解決するには、ステップ2とステップ3を確認します。

4.4. Catalyst Centerはトラストポイントと証明書を作成しませんでした sdn-network-infra-iwan。

- この問題を解決するには、ステップ2とステップ3を確認します。

4.5. Catalyst CenterはAssurance設定をプッシュしませんでした。

- このコマンド `show network-assurance summary` では、Network-Assuranceが次のように表示されま  
Disabledす。

```
<#root>
```

```
DC9800-WLC#
```

```
show network-assurance summary
```

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

- Catalyst Centerで設定をプッシュするために必要なデバイスコントロール機能がWLCで有効になっていることを確認します。デバイスの制御可能性は、ディスクバリプロセスでイネーブルにすることも、WLCがインベントリに登録され、Catalyst Centerによって管理された後にイネーブルにすることもできます。ページに移動し `Inventory` ます。を選択 `Device > Actions > Inventory > Edit Device > Device Controllability > Enable` します。

4.6. Catalyst Centerは、テレメトリサブスクリプションの設定をプッシュしません。

- コマンドを使用して、WLCにサブスクリプションがあることを確認し `show telemetry ietf subscription all` ます。
- そうでない場合は、ステップ2とステップ3を確認して、この問題を解決します。

4.7. WLCとCatalyst Center間のTLSハンドシェイクは、Catalyst Center証明書がWLCで検証できないため失敗します。

これは多くの理由が考えられます。最も一般的な理由を次に示します。

4.7.1. Catalyst Centerの証明書が期限切れであるか失効しているか、サブジェクト代替名(SAN)にCatalyst CenterのIPアドレスが含まれていない。

- 証明書が『[Catalyst Centerセキュリティのベストプラクティスガイド](#)』で指定されているベストプラクティスに一致していることを確認します。

4.7.2. 証明書失効リスト(CRL)を取得できないため、失効チェックが失敗する。

- DNSの障害、ファイアウォールの問題、WLCとCRL分散ポイント(CDP)間の接続の問題、次の既知の問題の1つなど、CRLの取得が失敗する原因は数多くあります。
  - Cisco Bug ID [CSCvr41793](#):PKI:CRLの取得でHTTP Content-Lengthが使用されません
  - Cisco Bug ID [CSCvo03458](#):CRLに到達できない場合、PKIの「revocation check crl none」がフォールバックしません。
  - Cisco Bug ID [CSCue73820](#):PKIデバッグでCRL解析の失敗が明らかにならない。
- 回避策として、DNAC-CAトラストポイントrevocation-check noneの下で設定を行います。

#### 4.7.3.証明書エラー「Peer certificate chain is too long to be verified」

- コマンドの出力を確認しshow platform software trace message mdt-pubd chassis active Rます。
- これが表示された場合は、次の点を確認し"Peer certificate chain is too long to be verified"します。

Cisco Bug ID [CSCvw09580](#):9800 WLCは4以上のCisco DNA Center証明書チェーンを使用しません。

- これを修正するには、次のコマンドを使用して、Catalyst Center証明書を発行した中間CAの証明書をWLCのトラストポイントにインポートします。echo | openssl s\_client -connect

```
:443 -showcerts
```

---

 注：これにより、信頼チェーン内の証明書のリスト（PEMエンコード済み）が生成されるので、各証明書は-----BEGIN CERTIFICATE-----で始まります。「回避策」セクションに記載されているURLを参照し、DNAC-CA証明書を設定する手順を実行します。ただし、ルートCA証明書はインポートしないでください。代わりに、問題のあるCAの証明書をインポートします。

---

#### 4.7.4. WLC証明書の期限切れ

- Catalyst Centerのバージョンが1.3.3.7以前の場合は、WLC証明書が期限切れになっている可能性があります。Catalyst Centerのバージョンが1.3.3.8以降の場合（2.1.2.6以降ではない場合）、バージョン1.3.3.7以前からのアップグレードの前に証明書が期限切れになっている場合は、問題が発生する可能性があります。
- コマンドの出力で有効期間の終了日を確認しshow crypto pki certificates sdn-network-infra-iwan Rます。

4.8. Catalyst Centerのcollector-iosxeサービスは、インベントリマネージャサービスによって新しいデバイスが通知されなかったため、WLCからの接続を受け入れません。

- iosxe-collectorによって認識されるデバイスのリストを確認するには、Catalyst Center CLIで次のコマンドを入力します。

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

- ホスト名とIPアドレスのリストだけを取得するには、次のコマンドを使用してjqで出力を解析します。

Catalyst Center 1.3以降 :

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

Catalyst Center 1.3.1以前 :

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

- このリストにWLCが含まれていない場合は、collector-iosxeサービスを再起動して、問題が解決するかどうかを確認します。
- collector-iosxeだけを再起動しても解決しない場合は、collector-managerサービスを再起動するとこの問題を解決できます。



ヒント : サービスを再起動するには、 `magctl service restart -d`

- 
- コマンドの出力がまだ表示さ `show telemetry internal connection` れている場合 "Connecting" は、collector-iosxeログにエラーを記録します。



ヒント : ログファイルを追跡するには、 `magctl service logs -rf` コマンドを入力します。この場合は、 `magctl service logs -rf collector-iosxe | lq`。

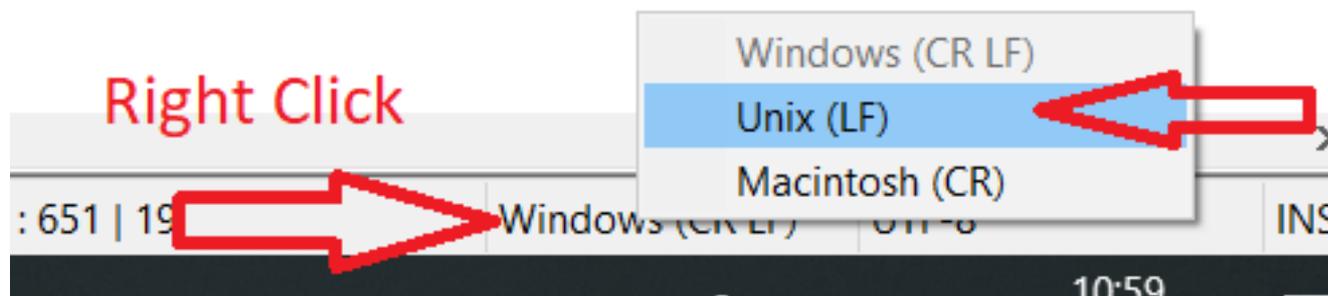
---

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

- このエラーが表示された場合は、Catalyst Centerに追加された証明書(.keyファイルと .pem ( 証明書チェーン ) ファイルの両方)をメモ帳++で開きます。メモ帳++で、に移動し `View > Show Symbol > Show All Characters` ます。
- 次のような場合です。

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIDzjCCArYCAQAwgcQxCzAJBgNVBAYTAkdCMRIwEAYDVQQIDAlCZXJrc2hpcmUx  
EDA0BgNVBAcMB1JlYWRpbmcxGTAXBgNVBAoMEFZpcmdpbmIjBNZWRpYSBMdGQxGzAZ  
BgNVBAsMEkNvcnBvcnF0ZSBOZXR3b3JrczEiMCAGAlUEAwWZY29ycC1kbmFjLnN5  
c3RlbXMucHJpdmF0ZTEzMDEGCSqGSIb3DQEJARYkY29ycG9yYXR1Lm51dHdvcmtz  
QHZpcmdpbm1lZG1hLmNvLnVrMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC  
AQEAqZlPszGCafwuoadcloR+yNIE6jl6/7VbzXDF5Ay5Lq9pU9KLFTpFnPV5jxDK  
8y0blhIqSf7cXxNZzi0SCRcGrw8M4ZWjC1DBY1FNJUfZQJaJSDkL/k/975udSJ7p  
HrDipMOBJzyZQxkpy3Rwem9vsr3De6hrYvo2t4wq8vTznPLUr48TQDdy89avkNbb  
FaVwGyxCsIxqE5LR/es/L/LPEBQm8v4ph8yi9F/Yqm2rECLw9QAIWhhyVjDC0Bc/  
kUjfYVvwaQH0eKCMELMi726zaTZs8woyL2clA037VxLfSuEz51F7hLtP5kxuTvFw  
a9zfhCxU+7MelY4po0VxthoOrQIDAQABoIHDMIHABgkqhkiG9w0BCQ4xgbIwga8w  
CQYDVR0TBAlwADALBgNVHQ8EBAMCBeAwgZQGA1UdEQSBjDCBiYIZY29ycC1kbmFj  
LnN5c3RlbXMucHJpdmF0ZiYIY29ycC1kbmFjghlwbmBzZXJ2ZXIuc3lzdGVtcy5w  
cm12YXR1hwQKSAXLhwQKSAXMhwQKSAXNhwQKSAXOhwQKS8BhwQKS8ChwQKS8D  
hwQKS8EhwQKS8+BhwQKS8+ChwQKS8+DhwQKS8+EMA0GCSqGSIb3DQEBCwUAA4IB  
AQAvWQKknbwYf5VcnoGTvQIsoIjyW/kQ438UW7gP2XOXoamxgxo/iGApo+bXpCW6  
MUXgYWos9Yg02cmDVV8aKqbCUt0QnaEsybJbrXqW33ZBKL1LqjFgSX/Ngte6TsAm  
ZoLYHqKrC6vjCfYqRVvWs7JA5Y3WjUknoRfg0AIB7LxPSADh7df8aoiG6gCANNWQs  
N8FdVJpT4zVivYLilBvq3TCqN946h7FxtxU4mKCh1VfUqM5sL7hTuOCvjq2PQ6mx  
ZuEHEh0vywgnV/aaGmKPbrbRA9gzoXkmCfdiDBhK/aLXCKXqoLsXe5zgCUaYLXTb  
nmPxUJEmlYrKdf9nc4TTVFhZ  
-----END CERTIFICATE REQUEST-----
```

次のページに移動します。



証明書を保存します。

- これらのスイッチをCatalyst Centerに再度追加し、コマンドが次のように表示されshow telemetry internal connectionかどうかを確認し"Active"ます。

#### 4.9. 関連不具合:

- Cisco Bug ID [CSCvs78950](#):eWLCからWolverineクラスタテレメトリへの接続が「Connecting」状態。
- Cisco Bug ID [CSCvr98535](#):Cisco DNA CenterでPKIのHTTPソースインターフェイスが設定されない – eWLCテレメトリが「Connecting」のままになる

ステップ 5 : テレメトリの状態はアクティブですが、Assuranceにはデータが表示されません。

次のコマンドを使用して、テレメトリの内部接続の現在のステータスを確認します。

```
<#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
```

考えられる不具合:

- Cisco Bug ID [CSCvu27838](#):eWLCを使用する9300からのワイヤレス保証データがありません。
- Cisco Bug ID [CSCvu00173](#):1.3.3.4へのアップグレード後、アシュアランスAPIルートが登録されない ( eWLC固有ではない ) 。

## 回避策

必要な設定の一部またはすべてがWLCにない場合は、なぜ設定が存在しないのかを判断します。不具合に一致するログファイルがあるかどうかを確認します。その後、回避策としてこれらのオプションを検討してください。

### Catalyst Centerバージョン2.x

Catalyst CenterのGUIで、ページに移動しInventoryます。を選択しWLC > Actions > Telemetry > Update Telemetry Settings > Force Configuration Push > Next > Applyます。その後、WLCが再同期プロセスを完了するまで少し待ちます。このドキュメントの「背景説明」セクションで説明されている設定がCatalyst Centerによってプッシュされることを確認し、コマンドを使用して、WLCにAssurance設定が存在することを確認しshow network-assurance summaryます。

### Catalyst Centerバージョン1.x

これは、以前のGUI方式で望ましい効果が得られない場合に、Catalyst Center 2.xでも使用できます。

- トラストポ<sup>s</sup>sdn-network-infra-iwanイントまたは証明書が失われています。

Catalyst Center Assuranceの証明書とサブスクリプションを手動でインストールするには、Cisco Technical Assistance Center(TAC)にお問い合わせください。

- ネットワーク保証の設定が存在しません。

Catalyst CenterエンタープライズVIPアドレスがWLCから到達可能であることを確認します。次に、次の例に示すように、このセクションを手動で設定します。

```
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:5行目で、X.X.X.Xと/ca/の間のスペースと/ca/とpemの間のスペースに注目してください。

---

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。