# 排除Cisco Catalyst Center上WLC 9800中的無保 證資料故障

目錄
<u>必要條件</u>
採用元件
<u>背景資訊</u>
對Catalyst Center上WLC的無保證資料進行故障排除
因應措施
<u>Catalyst中心版本2.x</u>
<u>Catalyst中心版本1.x</u>

## 簡介

本檔案將說明如何在Cisco Catalyst Center未顯示Catalyst 9800系列無線LAN控制器(WLC)的任何 保證資料時進行疑難排解。

## 必要條件

需求

思科建議您瞭解以下主題:

- Catalyst Center CLI的使maglev用
- 基本Linux基礎
- Catalyst Center和Catalyst 9800平台上的證書知識

### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Catalyst Center裝置第1代或第2代,軟體版本為1.x或2.x,帶有保證包
- Catalyst 9800系列WLC

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設) )的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

註:雖然最初為Catalyst Center 1.x編寫此文檔,但大多數文檔都適用於Catalyst Center 2.x。

✤ 註:Catalyst 9800 WLC必須已由Catalyst Center發現並分配給站點,且必須運行相容的Cisco IOS<sup>® XE</sup>版本。有關互通性的更多詳細資訊,請參閱<u>Catalyst Center相容性表</u>。

## 背景資訊

發現過程中, Catalyst Center會將下一個配置推送到WLC。

◆ 註:此範例來自Catalyst 9800-CL雲端無線控制器。使用實體Catalyst 9800系列裝置時,某些 詳細資訊可能會有所不同;X.X.X.X是Catalyst Center企業介面的虛擬IP(VIP)位址,而 Y.Y.Y是WLC的管理IP位址。

#### <#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

## 對Catalyst Center上WLC的無保證資料排除故障

步驟 1.確認WLC可連線並在Catalyst Center清單中管理。

如果WLC未處於「託管」狀態,則在繼續操作之前,您必須解決可接通性或配置問題。

❥┛提示:檢查清單管理器、spf-device-manager和spf-service-manager日誌以識別故障。

步驟 2.驗證Catalyst Center是否將所有必要的配置推送到WLC。

使用以下命令確保「背景資訊」一節中提到的組態已推送到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

已知的問題:

- 思科錯誤ID CSCvs62939 發現後, Cisco DNA Center不會將遙測配置推送到9xxx交換機。
- 思科錯誤ID <u>CSCvt83104</u> 如果裝置上存在Netconf候選資料儲存,則eWLC保證配置推送失 敗。
- 思科漏洞ID CSCvt97081 eWLC DNAC-CA憑證布建無法用於透過DNS名稱發現的裝置。

要驗證的日誌:

- dna-wireless-service 用於DNAC-CA證書和遙測配置。
- network-design-service 用於sdn-network-infra-iwan證書。

步驟 3.確認已在WLC上建立所需的憑證。

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

#### 已知問題和限制:

- Cisco錯誤ID <u>CSCvu03730</u> eWLC在Cisco DNA Center中未受到監控,因為未安裝sdnnetwork-infra-iwan證書(根本原因是pki-broker客戶端證書已過期)。
- 思科漏洞ID CSCvr44560 增強版:新增對IOS-XE在2099年後到期的CA證書的支援
- 思科漏洞ID CSCwc99759 增強版:新增對8192位RSA證書簽名的支援

#### 步驟 4.驗證遙測連線狀態。

使用以下命令確保遙測"Active"連線在WLC上處於狀態:

#### <#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Cisco IOS XE 17.7版及更高版本:

#### <#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

Connection up

X.X.X.X IP地址必須是Catalyst Center Enterprise介面。如果為Catalyst Center配置了VIP,則它必 須是企業介面的VIP。如果IP地址正確且狀態為"Active"正確,請繼續執行下一步。

如果狀態為"Connecting"此,則無法成功建立從WLC到Catalyst Center的超文字傳輸協定安全 (HTTPS)連線。這可能有許多不同的原因,下面列出了最常見的原因。

4.1. 無法從WLC訪問Catalyst Center VIP或處於狀"DOWN"態。

- 在具有VIP的單個節點上,當群集介面關閉時,VIP會關閉。驗證群集介面是否已連線。
- 確認WLC連線到企業VIP(ICMP/ping)。
- 使用以下命令驗證Catalyst Center Enterprise "UP" VIP是否處於狀態: ip a | grep en。
- 使用以下命令驗證Catalyst Center Enterprise VIP是否配置正確: etcdctl get /maglev/config/cluster/cluster\_network。

4.2. WLC處於高可用性(HA)狀態,故障轉移後,Assurance不起作用。

如果HA不是由Catalyst Center形成的,則會發生這種情況。在這種情況下:從清單中移除WLC、中 斷HA、探索兩個WLC,並讓Catalyst Center形成HA。

💊 註:此要求可在較新Catalyst Center版本中更改。

4.3. Catalyst Center未建立DNAC-CA信任點和證書。

• 檢查步驟2和步驟3。解決此問題。

4.4. Catalyst Center未建立信任點sdn-network-infra-iwan和證書。

• 請檢查步驟2.和步驟3以解決此問題。

4.5. Catalyst Center未推送保證配置。

• 命令將show network-assurance summaryNetwork-Assurance顯示為Disabled:

#### <#root>

DC9800-WLC#

show network-assurance summary

------ Network-Assurance :

#### Disabled

Server Url		:
ICap Server Port Number	:	
Sensor Backhaul SSID		:
Authentication		: Unknown

• 確保WLC已啟用裝置可控性,因為Catalyst Center推送配置需要此功能。可以在發現過程中 啟用裝置可控性,或者在WLC位於清單上並由Catalyst Center管理後啟用裝置可控性。導航 到頁 Inventory面。選Device > Actions > Inventory > Edit Device > Device Controllability > Enable擇。

4.6. Catalyst Center不推送遙測訂閱配置。

- 使用命令確保WLC具有訂show telemetry ietf subscription all用。
- 如果不是,請檢查步驟2和步驟3以解決此問題。

4.7. WLC和Catalyst Center之間的TLS握手失敗,因為WLC無法驗證Catalyst Center證書。

這可能是由於多種原因,下面列出了最常見的原因:

4.7.1. Catalyst Center證書已過期或吊銷,或者主體替代名稱(SAN)中沒有Catalyst Center IP地址。

- 確保證書與Catalyst Center安全最佳實踐指南中指定的最佳實踐相匹配。
- 4.7.2.撤銷檢查失敗,因為無法檢索證書撤銷清單(CRL)。
  - CRL檢索失敗的原因可能很多,例如DNS故障、防火牆問題、WLC和CRL分發點(CDP)之間 的連線問題,或者以下已知問題之一:
    - 。思科錯誤ID CSCvr41793 PKI:CRL檢索不使用HTTP Content-Length。
    - ◎ 思科錯誤ID <u>CSCvo03458</u> 如果無法訪問CRL,則PKI「revocation check crl none」 不會回退。
    - <sup>。</sup>思科錯誤ID <u>CSCue73820</u> PKI調試不明確關於CRL分析失敗。
  - 作為解決方法,revocation-check none請在DNAC-CA信任點下配置。

4.7.3.證書錯誤「對等證書鏈過長,無法驗證」。

- 檢查命令的輸show platform software trace message mdt-pubd chassis active R出。
- 如果這顯示, "Peer certificate chain is too long to be verified"請檢查:

思科漏洞ID CSCvw09580 - 9800 WLC不會將Cisco DNA Center證書鏈深度設定為4或更多。

• 若要解決此問題,請使用以下命令,將核發Catalyst Center憑證的中間CA的憑證匯入WLC上 的信任點echo | openssl s\_client -connect

:443 -showcerts

:.

◆ 注意:這會產生信任鏈(PEM編碼)中的證書清單,因此每個證書以-----BEGIN CERTIFICATE」開-----。請參閱「解決方法」部分中提到的URL,並執行用於配置DNAC-CA證書的步驟,但不要匯入根CA證書。相反,請匯入有問題的CA的證書。

4.7.4. WLC證書已過期。

當Catalyst Center的版本是1.3.3.7或更低版本時,WLC證書可能已過期。當Catalyst Center的版本是1.3.3.8或更高版本(但不是2.1.2.6或更高版本)時,如果證書在從版本1.3.3.7或更低版本升級之前過期,則仍會出現此問題。

• 檢查命令輸出中的有效結束日show crypto pki certificates sdn-network-infra-iwan期。

4.8. Catalyst Center上的收集器iosxe服務不接受來自WLC的連線,因為清單管理器服務沒有通知它 新裝置。

• 若要檢查iosxe-collector已知裝置的清單,請在Catalyst Center CLI上輸入以下命令:

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

• 為了隻獲取主機名和IP地址清單,請使用以下命令使用jq分析輸出:

在Catalyst Center 1.3及更高版本上:

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

在Catalyst Center 1.3.1及更低版本上:

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

- 如果此清單不包含WLC,則重新啟動收集器iosxe服務,並確認這是否解決了問題。
- 如果單獨重新啟動收集器iosxe不起作用,則重新啟動收集器 管理器服務有助於解決此問題

ک 提示:若要重新啟動服務,請輸magetl service restart -d 入。

• 如果命令的輸出仍然show telemetry internal connection存在, "Connecting" 請跟蹤錯 collector-iosxe 誤的日誌:

提示:要跟蹤日誌檔案,請輸入命magctl service logs -rf 令。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.KeyStor at java.util.Base64\$Decoder.decode0(Base64.java:714)
- 如果您看到此錯誤,請在記事本++中開啟已新增到Catalyst Center的憑證,包括其.key和.pem(憑證鏈結)檔案。在記事本++中,導航到View > Show Symbol > Show All Characters。
- 如果你有這樣的東西:

0

----BEGIN · CERTIFICATE · REQUEST-----MIIDzjCCArYCAQAwgcQxCzAJBgNVBAYTAkdCMRIwEAYDVQQIDA1CZXJrc2hpcmUxCR EDAOBgNVBAcMB1J1YWRpbmcxGTAXBgNVBAoMEFZpcmdpb1BNZWRpYSBMdGQxGzAZCR BgNVBAsMEkNvcnBvcmF0ZSB0ZXR3b3JrczEiMCAGA1UEAwwZY29ycC1kbmFjLnN5CRIF c3R1bXMucHJpdmF02TEzMDEGCSqGSIb3DQEJARYkY29ycG9yYXR1Lm51dHdvcmtzCR QHZpcmdpbmllZGlhLmNvLnVrMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC AQEAqZ1PszGCafwuoadcloR+yNIE6j16/7VbzXDF5Ay5Lq9pU9KLFTpFnPV5jxDKCR 8y0blhIqSf7cXxNZZi0SCRcGrw8M4ZWjC1DBY1FNJUfZQJaJSDkL/k/975udSJ7pCR HrDIpMOBJzyZQxkpy3Rwem9vsr3De6hrYvo2t4wq8vTznPLUr48TQDdy89avkNbb FaVwGyxCsIxqE5LR/es/L/LPEBQm8v4ph8yi9F/Yqm2rECLw9QAiWhhyVjDC0Bc/CBC kUjfYVwwaQH0eKCMeLMi726zaTZs8woyL2clA037VxLfSuEz51F7hLtP5kxuTvFwCRDE a9zfhCxU+7Me1Y4po0VxthoOrQIDAQABoIHDMIHABgkqhkiG9w0BCQ4xgbIwga8w CQYDVR0TBAIwADALBgNVHQ8EBAMCBeAwgZQGA1UdEQSBjDCBiYIZY29ycC1kbmFj CRIE LnN5c3RlbXMucHJpdmF0ZYIJY29ycC1kbmFjgh1wbnBzZXJ2ZXIuc31zdGVtcy5w cm12YXR1hwQKSAXLhwQKSAXMhwQKSAXNhwQKSAXOhwQKSn8BhwQKSn8ChwQKSn8DCR hwQKSn8EhwQKSn+BhwQKSn+ChwQKSn+DhwQKSn+EMA0GCSqGSIb3DQEBCwUAA4IBCR AQAvWQKknbwYf5VcnoGTvQIsoIjyW/kQ438UW7gP2XOXoamxgxo/iGApo+bXpCW6 MUXgYWos9Yg02cmDVV8aKqbCUt0QnaEsybJbrXqW33ZBKL1LqjFgSX/Ngte6TsAm 🖼 💷 ZoLYHqKrC6vjCfYqRVvWs7JA5Y3WjUknoRfq0AIB7LxPSADh7df8aoiG6qCNNWQsCRIE N8FdVJpT4zVivYLi1Bvq3TCqN946h7FxtxU4mKcH1VfUqM5sL7hTuOCvjqZPQ6mxCRLF ZuEHEh0vywgnV/aaGmKPbrbRA9gzoXkmCfdiDBhK/aLXCKXqoLsXe5zgCUaYLXTbCR nmPxUJEmlyrKDf9nc4TTVFhZCRUE ---END · CERTIFICATE · REQUEST ---- CRLF

然後轉到:



### 並儲存證書。

• 將它們再次新增到Catalyst Center,並檢查命令現在show telemetry internal connection是否顯示 "Active"。

### 4.9.相關缺陷:

- 思科漏洞ID <u>CSCvs78950</u> eWLC到Wolverine群集遙測連線處於「Connecting」狀態。
- 思科錯誤ID <u>CSCvr98535</u> Cisco DNA Center不為PKI配置HTTP源介面 eWLC遙測保持「 連線」。

步驟 5.遙測狀態處於活動狀態,但在保證中仍看不到任何資料。

使用以下命令驗證遙測內部連線的當前狀態:

<#root>

dna-9800#

show telemetry internal connection

Telemetry connection

Active

sdn-network-infra-iwan

可能的缺陷:

- 思科錯誤ID CSCvu27838 使用eWLC的9300無無線保證資料。
- 思科錯誤ID CSCvu00173 升級到1.3.3.4後未註冊保證API路由(非特定於eWLC)。

## 因應措施

如果所需的部分或全部組態不在WLC中,請嘗試判斷為什麼組態不存在。如果存在缺陷匹配項,請 檢查相關日誌檔案。然後,將這些選項視為一種變通辦法。

Catalyst中心版本2.x

在Catalyst Center GUI上,導航到頁Inventory面。選擇WLC > Actions > Telemetry > Update Telemetry Settings > Force Configuration Push > Next > Apply。程式完成後,請等待一段時間,直到WLC完成重新同步程式。確認Catalyst Center會推送本檔案「背景資訊」一節中提到的組態,並透過命令驗證WLC上是否存在保證組show network-assurance summary態。

Catalyst中心版本1.x

如果先前的GUI方法仍然沒有達到預期效果,則此命令也可用於Catalyst Center 2.x。

• 信任sdn-network-infra-iwan點和/或證書丟失。

請聯絡思科技術協助中心(TAC),以手動安裝Catalyst Center保證證書和訂閱。

• 網路保證配置不存在。

確保可以從WLC訪問Catalyst Center企業VIP地址。然後手動配置該部分,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 PROTCOL\_HTTP X.X.X.X /ca/ pem

≫ 註:在第五行,記下X.X.X.X和/ca/之間的空格以及/ca/和pem之間的空格。

### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。