

# 使用WLC排除CMX連線故障

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[排除可能的故障情況](#)

[驗證可達性](#)

[時間同步](#)

[SNMP連線能力](#)

[NMSP可達性](#)

[版本相容性](#)

[控制器上推送的正確雜湊值](#)

[控制器端AireOS上不存在雜湊](#)

[控制器端聚合接入IOS-XE上不存在雜湊](#)

## 簡介

本檔案介紹對無線LAN控制器(WLC)的連線問題進行疑難排解的方法，此控制器既是整合式控制器，也是使用連線行動體驗(CMX)進行融合器。

## 必要條件

### 需求

思科建議您瞭解配置流程和部署指南。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CMX 10.2.3-34
- WLC 2504/8.2.141.0
- 虛擬WLC 8.3.102.0
- 融合接入WLC C3650-24TS/03.06.05E

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。

附註：如果您使用的是CMX 10.6，則需要安裝特殊的修補程式才能切換到root使用者。請聯絡Cisco TAC進行安裝。

此外，在某些情況下，即使有根修補程式，也需要使用完整路徑執行命令，例如"/bin/snmpwalk ..."

以防萬一「snmpwalk」不起作用。

## 背景資訊

本文重點介紹以下情況：將WLC新增到CMX後出現故障，或者WLC顯示為無效或非活動。基本上，當網路移動服務協定(NMSP)隧道未啟動或NMSP通訊顯示為非活動時。

WLC和CMX之間的通訊使用NMSP進行。

NMSP在面向WLC的TCP埠16113上運行並基於TLS，後者要求在移動服務引擎(MSE)/CMX和控制器之間進行證書(金鑰雜湊)交換。控制器會啟動WLC和CMX之間的傳輸層安全/安全套接字層(TLS/SSL)隧道。

## 排除可能的故障情況

首先使用此命令輸出。

登入到CMX命令列並運行命令 `cmxctl config controllers show`。

```
** To troubleshoot INACTIVE/INVALID controllers verify that:  
the controller is reachable  
the controller's time is same or ahead of MSE time  
the SNMP port(161) is open on the controller  
the NMSP port(16113) is open on the controller  
the controller version is correct  
the correct key hash is pushed across to the controller by referring the following:  
+-----+  
| MAC Address      | 00:50:56:99:47:61 |  
|  
+-----+  
| SHA1 Key         | f216b284ba16ac827313ea2aa5f4dec1817f1069 |  
+-----+  
| SHA2 Key         | 2e359bd5e83f32c230b03ed8172b33652ce96c978e2733a742aaa3d47a653a02 |  
+-----+
```

此外，CMX MAC地址和Hash-key可從輸出中找到：

當至少有一個非活動項時，輸出會顯示一個清單：

1. 可達性
2. 時間
3. 簡易網路管理通訊協定(SNMP)161連線埠
4. NMSP 16113埠
5. 版本
6. 控制器上推送的正確雜湊

## 驗證可達性

若要檢查與控制器的連線能力，請從CMX對WLC執行ping。

## 時間同步

最佳作法是將CMX和WLC指向同一個網路時間協定(NTP)伺服器。

在整合WLC(AireOS)中，使用以下命令設定：

```
config time ntp server <index> <IP address of NTP>
```

在融合接入IOS-XE中，運行命令：

```
(config)#ntp server <IP address of NTP>
```

若要更改CMX中NTP伺服器的IP地址（在CMX 10.6之前）：

步驟1.以cmxadmin身份登入命令列，切換到root用戶<su root>。

步驟2.使用cmxctl stop -a指令停止所有CMX服務。

步驟3.使用命令service ntpd stop停止NTP解調。

步驟4.停止所有進程後，運行命令vi /etc/ntp.conf。按一下i以切換到插入模式並更改IP地址，然後按一下ESC並鍵入:wq以儲存配置。

步驟5.更改引數後，運行命令service ntpd start。

步驟6.使用ntpdate -d <NTP server的IP地址>命令檢查是否可以訪問NTP伺服器。

步驟7.至少等待5分鐘，以便使用ntpstat命令重新啟動NTP服務並進行驗證。

步驟8.在NTP伺服器與CMX同步後，運行命令cmxctl restart重新啟動CMX服務並切換回cmxadmin用戶。

在CMX 10.6之後，您可以通過以下方式驗證和更改CMX NTP配置：

步驟1.以cmxadmin身份登入命令列

步驟2.檢查NTP與cmxos運行狀況的NTP同步

步驟3. 如果要重新配置NTP伺服器，可以使用cmxos ntp clear，然後使用cmxos ntp type。

步驟4.在NTP伺服器與CMX同步後，運行命令cmxctl restart重新啟動CMX服務並切換回cmxadmin用戶。

## SNMP連線能力

若要檢查CMX是否可存取SNMP到WLC，請在CMX中執行命令：

```
Snmpwalk -c <name of community> -v 2c <IP address of WLC>.
```

此命令假設WLC執行預設的SNMP版本2。在版本3中，命令如下所示：

```
snmpwalk -v3 -l authPriv -u <snmpadmin> -a SHA -A <password> -x AES -X <PRIVPassWord>  
127.0.0.1:161 system
```

如果SNMP未啟用，或社群名稱錯誤，則超時。如果成功，則會看到WLC的整個SNMP資料庫內容。

**附註：**如果CMX與WLC服務埠位於同一子網中，則無法在CMX與WLC之間建立連線。

## NMSP可達性

若要檢查CMX是否可以訪問WLC的NMSP，請運行以下命令：

在CMX中：

```
netstat -a | grep 16113
```

在WLC中：

```
show nmsp status  
show nmsp subscription summary
```

## 版本相容性

檢查版本與最新文檔的相容性。

<http://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html#pgflid-229490>

## 控制器上推送的正確雜湊值

### 控制器端AireOS上不存在雜湊

通常wlc自動新增sha2和使用者名稱。這些金鑰可以使用**show auth-list**指令驗證。

```
(Cisco Controller) >show auth-list
```

```
Authorize MIC APs against Auth-list or AAA ..... disabled  
Authorize LSC APs against Auth-List ..... disabled  
APs Allowed to Join  
  AP with Manufacturing Installed Certificate.... yes  
  AP with Self-Signed Certificate..... no  
  AP with Locally Significant Certificate..... no
```

```
Mac Addr          Cert Type      Key Hash  
-----  
00:50:56:99:6a:32  LBS-SSC-SHA256  
7aa0d8facc0aa4a5a65b374f7d16972d142f4bb4823d91b7bc143811c7534e32
```

如果表中沒有CMX的雜湊金鑰和MAC地址，則可以在WLC中手動新增：

```
config auth-list add sha256-lbs-ssc <mac addr of CMX> <sha2key>
```

### 控制器端聚合接入IOS-XE上不存在雜湊

在NGWC控制器中，需要手動運行命令，如下所示：

```
nmsp enable
username<cmx mac-addr> mac aaa attribute list <list name>
aaa attribute list CMX
attribute type password <CMX sha2 key >
```

**附註：**必須新增cmx mac-addr，不帶標點符號冒號(:)

若要疑難排解雜湊關鍵字：

```
Switch#show trace messages nmsp connection
```

```
[12/19/16 14:57:50.389 UTC 4dd 8729] sslConnectionInit: SSL_do_handshake for conn ssl 587c85e0,
conn state: INIT, SSL state: HANDSHAKING
[12/19/16 14:57:50.395 UTC 4de 8729] Peer certificate Validation Done for conn ssl 587c85e0,
calling authlist..
[12/19/16 14:57:50.396 UTC 4df 8729] Client Cert Hash Key
[2e359bd5e83f32c230b03ed8172b33652ce96c978e2733a742aaa3d47a653a02]
[12/19/16 14:57:50.397 UTC 4e0 8729] Authlist authentication failed for conn ssl 587c85e0
[12/19/16 14:57:51.396 UTC 4e1 8729] Peer Not Validated against the AuthList
```

如果您仍然面臨任何問題，請訪問思科支**[援論壇](#)**尋求幫助。本文中提到的輸出和核對表肯定能幫助您縮小論壇上的問題範圍，或者您也可以提交一個TAC支援請求。