# 排除故障CMX与WLC的连接

## 目录



## 简介

本文分析方法排除故障连通性问题无线局域网控制器(WLC) ：统一和聚合与已连接移动经验(CMX)。它着重添加WLC到CMX出故障的情况或WLC出现如无效或非激活：基本上，当NMSP (网络移动性服务协议)通道不出来。

WLC和CMX之间的通信发生与使用NMSP。

NMSP在TCP端口16113运行往WLC和根据TLS，要求在MSE/CMX和控制器之间的证书(关键哈希)交换。在WLC和CMX之间的TLS/SSL通道由控制器发起。

## 先决条件

### 使用的组件

CMX 10.2.3-34

WLC 2504/8.2.141.0

虚拟WLC 8.3.102.0

聚合的访问WLC C3650-24TS/03.06.05E

### 要求

本文假设您已经熟悉配置过程和部署指南。它仅着重NMSP通信出现如非激活的故障排除情况

## 排除故障：可能的故障情景

开始的第一个地方是以下命令输出：

登陆在CMX line命令并且运行命令“cmxctl设置控制器显示”

```
** 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        |
+------------------+-------------------------------------------------------------------------+
```

并且，从输出您能发现CMX MAC地址和HASH KEY ：

输出，当有至少一个非激活，将显示清单：

1. 可接通性
2. 时间
3. SNMP 161端口
4. NMSP 16113端口
5. version
6. 更正在控制器推送的哈希

## 1- 验证可接通性

要检查可接通性到控制器请发出一ping从CMX对WLC

## 2时间同步

最佳实践是指向两CMX和WLC同样网络时间协议(NTP)服务器。

在Unified WLC (AireOS)这设置命令：

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

在聚合的访问IOS-XE ：

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

更改Ntp server的IP地址在CMX ：

1. 对line命令的登录作为cmxadmin，对root用户<su root>的交换机
2. 终止所有服务用命令“cmxctl的终止-”
3. 一旦所有进程被终止，请输入命令“vi /etc/ntp.conf” ：按“我”换成插入模式和更改IP地址，然后按“ESC”和键入“：”保存配置的wq;
4. 一旦参数更改，请发出命令“cmxctl重新启动”重新启动服务和交换机回到cmxadmin用户。

## 3-SNMP可接通性

要检查CMX是否能访问SNMP到WLC，请发出in命令CMX ：

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

上述命令假设WLC运行默认SNMP版本2.，万一使用仅版本3，命令将看起来象：

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

如果SNMP没有启用或者属性名称是错误的那里将是超时。如果成功，您将看到WLC的全部的SNMP数据库内容。

## 4-NMSP可接通性

要检查CMX是否能访问NMSP到WLC，请发出命令：

在CMX ：

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

在WLC ：

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

## 5版本兼容性

用最新的文档检查版本兼容性。

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

## 在控制器推送的6正确哈希

### 6a) 哈希不在控制器侧AireOS

通常， wlc自动地添加sha2和用户名，并且密钥可以用命令验证：显示验证管理列表

```
(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
```

如果哈希密钥和MAC地址CMX不是存在表里，则它手工是可能的添加在WLC ：

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

### 6b) 哈希不在控制器侧聚合访问IOS-XE

在NGWC控制器中您需要手工运行命令如下：

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

**注意：** cmx应该添加mac-addr，不用列(：)

排除故障哈希密钥：

```
 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
```

# 仍然有问题？

如果所有在上面不指向问题，感到自由访问为帮助的Cisco支持论坛(上述输出和清单明确地将帮助缩小您的在论坛的问题)或打开TAC支持请求!