排除故障CMX与WLC的连接

目录

简介

本文描述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)。

先决条件

要求

思科建议您有配置过程和部署指南的知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 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

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。如果您的网络实际，请保证您了解所有命令潜在影响。

背景信息

此条款着重WLC被添加到CMX的情况，并且发生故障，或者WLC出现如无效或非激活。基本上

，当网络移动性服务协议(NMSP)时通道不出来或NMSP通信出现如非激活。

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，要求在移动服务引擎(MSE) /CMX和控制器之间的证书(关键哈希)交换。在WLC和CMX之间的传输层安全/安全套接字协议层(TLS/SSL)通道由控制器发起。

排除故障可能的故障情景

开始的第一个地方是此命令输出。

登录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， CMX MAC地址和HASH KEY可以从输出被找到：

输出，当有至少一个非激活时，显示清单：

1. 可接通性
2. 时间
3. 简单网络管理协议(SNMP) 161端口
4. NMSP 16113端口
5. version
6. 更正在控制器推送的哈希

验证可接通性

为了检查可接通性到控制器，请运行ping从CMX到WLC。

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，请运行行命令：

```
(config)#ntp server <IP address of NTP>
```
为了更改Ntp server的IP地址在CMX ：

步骤1.登录line命令作为**cmxadmin**，交换机对root用户**<su root>**。

步骤2.终止与命令**cmxctl终止的**所有CMX服务**- a**。

步骤3.终止与service命令**ntpd终止的**NTP deamon。

第四步：一旦所有进程被终止，请运行vi命令**/etc/ntp.conf**。 点击**i**换成插入模式和更改IP地址，然后点击**ESC**和键入：保存配置的**wq**。

第五步：一旦参数更改请运行service命令**ntpd开始**。

第六步：检查Ntp server是否是可及的与命令**ntpdate - NTP server>的d < IP地址**。

步骤7.允许至少五分钟，为了NTP服务重新启动和验证与命令**ntpstat**。

步骤 8一旦Ntp server与CMX同步，请运行命令**cmxctl重新启动**重新启动CMX服务和交换机回到**cmxadmin**用户。

SNMP可接通性

为了检查CMX是否能访问SNMP到WLC，请运行in命令CMX ：

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

此命令假设WLC运行默认SNMP版本2。在版本3，命令看起来象：

```
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是超时。如果它是成功的，您看到WLC的全部的SNMP数据库内容。

NMSP可接通性

为了检查CMX是否能访问NMSP到WLC，请运行命令：

在CMX ：

```
 netstat -a | grep 16113
```
在WLC ：

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

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

更正在控制器推送的哈希

切细不现在控制器旁拉AireOS

通常， wlc自动地添加sha2和用户名。密钥可以验证与show命令**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>
```

哈希不在控制器旁拉聚合的访问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 >
```

Note:cmx必须添加mac-addr，不用标点符号冒号(：)

为了排除故障哈希密钥：

```
 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**

如果仍然面对任何问题，请访问为帮助的Cisco支持论坛。在此条款和清单提及的输出可明确地帮助您缩小您的在论坛的问题或您能打开TAC支持请求。