使用WLC排除CMX连接故障

目录

简介

本文档介绍排除无线局域网控制器(WLC)连接问题的方法，包括统一和融合互联移动体验(CMX)。

先决条件

要求

思科建议您了解配置流程和部署指南。

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
- 融合接入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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

注意：如果使用CMX 10.6，则需要安装特殊补丁才能切换到根用户。联系思科TAC安装。

此外，在某些情况下，即使有根补丁，您也需要使用完整路径执行命令，例如"/bin/snmpwalk..." 以防“snmpwalk”不起作用。

背景信息

本文重点介绍WLC被添加到CMX并失败，或WLC显示为无效或非活动的情况。基本上，当网络移动服务协议(NMSP)隧道未启动或NMSP通信显示为非活动状态时。

WLC和CMX之间的通信使用NMSP。

NMSP在TCP端口16113上向WLC运行，并基于TLS，这要求移动服务引擎(MSE)/CMX与控制器之间进行证书（密钥散列）交换。WLC和CMX之间的传输层安全/安全套接字层(TLS/SSL)隧道由控制器发起。

排除可能的故障场景

首先从此命令输出开始。

登录CMX命令行并运行命令**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，从输出中可以找到CMX MAC地址和散列密钥：

当至少有一个非活动状态时，输出将显示一个核对表：

1. 可达性
2. 时间
3. 简单网络管理协议(SNMP)161端口
4. NMSP 16113端口
5. 版本
6. 控制器上推送的正确哈希

检验可达性

要检查到控制器的可达性，请从CMX对WLC运行ping。

时间同步

最佳实践是将CMX和WLC指向同一网络时间协议(NTP)服务器。

在Unified WLC(AireOS)中，此设置使用命令：

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

在融合接入IOS-XE中，运行命令：

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

要更改CMX中NTP服务器的IP地址（在CMX 10.6之前）：

步骤1.以**cmxadmin**身份登录命令行，切换到根用户**<su root>**。

步骤2.使用命令cmxctl stop -a停止所**有CMX服务**。

步骤3.使用命令service ntpd stop停止NTP**调试**。

步骤4.停止所有进程后，运行命令**vi /etc/ntp.conf**。单击i切换以插入模式并更改IP地址，然后单击**ESC** 并键入**:wq**以保存配置。

步骤5.更改参数后，运行命令service **ntpd start**。

步骤6.使用命令ntpdate -d <NTP服务器的IP地址>检查**NTP服务器是否可达**。

步骤7.至少允许五分钟，NTP服务重新启动并使用命令**ntpstat**进行验证。

步骤8. NTP服务器与CMX同步后，运行命令**cmxctl restart**以重新启动CMX服务并切换回**cmxadmin**用户。

在CMX 10.6之后，您可以这样验证和更改CMX NTP配置：

步骤1.以cmxadmin身份登录命**令行**

步骤2.检查与cmxos运行状况ntp的**NTP同步**

第 3 步： 如果要重新配置NTP服务器，可以使用cmxos ntp clear **，然后**使用**cmxos ntp type**。

步骤4.一旦NTP服务器与CMX同步，请运行命令**cmxctl restart**以重新启动CMX服务并切换回**cmxadmin**用户。

SNMP可达性

要检查CMX是否可以访问WLC的SNMP，请在CMX中运行命令：

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

此命令假设WLC运行默认SNMP第2版。在第3版中，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未启用，或者社区名称错误，则超时。如果成功，您将看到WLC的整个SNMP数据库内容。

注意：如果CMX与WLC服务端口位于同一子网中，则CMX和WLC之间将不建立连接。

NMSP可达性

要检查CMX是否可以访问NMSP到WLC，请运行以下命令：

在CMX中：

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

在WLC中：

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

版本兼容性

检查与最新文档的版本兼容性。

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

控制器上推送的正确哈希

控制器端AireOS上不存在散列

通常，wlc会自动添加sha2和用户名。可使用命令show auth-list**来验证密钥**。

```
(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
```

如果表中不存在CMX的哈希密钥和MAC地址，则可以在WLC中手动添加：

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

控制器端融合接入IOS-XE上不存在散列

在NGWC控制器中，您需要手动运行以下命令：

```
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 mac-addr必须添加，不带标点符号冒号(:)

要排除散列密钥故障，请执行以下操作：

```
 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
```

如果您仍然遇到任何问题，请访问思科支持论坛寻求帮助。本文中提及的输出和核对表无疑可以帮助您缩小论坛上的问题范围，或者您可以提交TAC支持请求。