Troubleshoot CMX Connectivity with WLC

Contents

Introduction

This document describes the methods to troubleshoot the connectivity issues of Wireless LAN Controller (WLC), both Unified and Converged with Connected Mobile Experience (CMX).

Prerequisites

Requirements

Cisco recommends that you have knowledge of the configuration process and the deployment guide.

Components Used

The information in this document is based on these software and hardware versions:

- CMX 10.2.3-34
- WLC 2504 / 8.2.141.0
- virtual WLC 8.3.102.0
- Converged Access WLC C3650-24TS / 03.06.05E

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Note: if you are using CMX 10.6, you need to have to have a special patch installed in order to switch to root user. Contact Cisco TAC to have it installed.

Also, in some instances even with a root patch you need to execute the command using the full path, e.g. "/bin/snmpwalk ..." in case "snmpwalk" does not work.

Background Information

This article focuses on situations where a WLC is added to the CMX and it fails, or the WLC shows up as invalid or inactive. Basically when the Network Mobility Service Protocol (NMSP) tunnel doesn't come up or the NMSP communications shows up as Inactive.

The communication between the WLC and CMX happens with the use of NMSP.

NMSP runs on TCP port 16113 towards the WLC and based on TLS, which requires a certificate (key hash) exchange between Mobility Services Engine (MSE)/CMX and the controller. The Transport Layer Security/Secure Sockets Layer (TLS/SSL) tunnel between the WLC and CMX is initiated by the controller.

Troubleshoot Possible Failure Scenarios

The first place to start is with this command output.

Log into the CMX command line and run the command **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         |
+------------------+--------------------------------------------------------------------------+
```

Also, the CMX MAC address and Hash-key can be found from the output:

The output, when there is at least one inactive, shows a checklist:

1. Reachability
2. Time
3. Simple Network Management Protocol (SNMP) 161 port
4. NMSP 16113 port
5. Version
6. Correct Hash pushed on the controller

Verify Reachability

In order to check the reachability to the Controller, run a ping from CMX to the WLC.

Time Synchronization

The best practice is to point both CMX and the WLC to same Network Time Protocol (NTP) server.

In Unified WLC (AireOS), this is set with the command:

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

In converged access IOS-XE, run the command:

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

In order to change the IP address of NTP server in CMX (before CMX 10.6):

Step 1. Log into the command line as **cmxadmin**, switch to root user <**su root**>.

Step 2. Stop all the CMX services with the command **cmxctl stop -a**.

Step 3. Stop the NTP deamon with the command **service ntpd stop**.

Step 4. Once all the process are stopped, run the command **vi /etc/ntp.conf**. Click **i** to switch to insert mode and change the IP address, then click **ESC** and type **:wq** to save the configuration.

Step 5. Once the parameter is changed run the command **service ntpd start**.

Step 6. Check if the NTP server is reachable with the command **ntpdate -d <IP address of NTP server>**.

Step 7. Allow five minutes at least, for the NTP service to restart and verify with the command **ntpstat**.

Step 8. Once the NTP server is synchronized with CMX, run the command **cmxctl restart** to restart the CMX services and switch back to **cmxadmin** user.

After CMX 10.6, you can verify and change the CMX NTP configuration this way :

Step 1. Log into the command line as **cmxadmin**

Step 2. Check the NTP synchronization with **cmxos health ntp**

Step 3. If you want to reconfigure the NTP server, you can use **cmxos ntp clear** and then **cmxos ntp type**.

Step 4. Once the NTP server is synchronized with CMX, run the command **cmxctl restart** to restart the CMX services and switch back to **cmxadmin** user.

SNMP Reachability

In order to check if CMX can access SNMP to the WLC, run the command in CMX:

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

This command assumes the WLC runs the default SNMP version 2. In version 3, the command looks like :

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

If SNMP is not enabled, or the community name is wrong there is a timeout. If it is successful, you see the whole SNMP database content of the WLC.

> **Note**: Connection between CMX and WLC will not be established if CMX is in the same subnet as WLC service port.

NMSP Reachability

In order to check if CMX can access NMSP to the WLC, run the commands:

In CMX:

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

In the WLC:

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

Version Compatibility

Check the version compatibility with the latest document.

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

Correct Hash Pushed on Controller

Hash Not Present on Controller Side AireOS

Usually, the wlc automatically adds the sha2 and username. The keys can be verified with the command **show auth-list**.

```
(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
```

If the hash key and MAC address of CMX are not present in table, then it is possible to add manually in WLC:

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

Hash Not Present on Controller Side Converged Access IOS-XE

In NGWC controllers, you need to run the commands manually as follows:

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

Note: cmx mac-addr must be added without punctuation mark colon (:)

In order to troubleshoot the hash key:

```
 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
```

If you still face any issues, visit cisco support forums for help. The outputs and checklist mentioned in this article can definitely help you narrow down your problem on the forums or you can open a TAC support request.