Fehlerbehebung bei CMX-Verbindungen mit WLC

Inhalt

Einführung

Dieses Dokument beschreibt die Methoden zur Behebung von Verbindungsproblemen beim Wireless LAN Controller (WLC), sowohl bei Unified als auch bei Converged with Connected Mobile Experience (CMX).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse des Konfigurationsprozesses und des Bereitstellungsleitfadens zu verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- CMX 10.2.3-34
- WLC 2504 / 8.2.141.0
- Virtual WLC 8.3.102.0
- Konvergenter Zugriff WLC C3650-24TS / 03.06.05E

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hinweis: Wenn Sie CMX 10.6 verwenden, müssen Sie einen speziellen Patch installieren, um zum Root-Benutzer zu wechseln. Wenden Sie sich für die Installation an das Cisco TAC.

In einigen Fällen müssen Sie den Befehl auch mit einem Root-Patch über den vollständigen Pfad ausführen, z.B. "/bin/snmpwalk ..." falls "snmpwalk" nicht funktioniert.

Hintergrundinformationen

Dieser Artikel behandelt Situationen, in denen ein WLC dem CMX hinzugefügt wird und fehlschlägt oder der WLC als ungültig oder inaktiv angezeigt wird. Im Prinzip, wenn der NMSP-Tunnel (Network Mobility Service Protocol) nicht verfügbar ist oder die NMSP-Kommunikation als inaktiv angezeigt wird.

Die Kommunikation zwischen WLC und CMX erfolgt mit der Verwendung von NMSP.

NMSP wird auf dem TCP-Port 16113 zum WLC ausgeführt und basiert auf TLS. Dies erfordert einen Zertifikataustausch (Schlüssel-Hash) zwischen Mobility Services Engine (MSE)/CMX und dem Controller. Der Transport Layer Security/Secure Sockets Layer (TLS/SSL)-Tunnel zwischen dem WLC und CMX wird vom Controller initiiert.

Fehlerbehebung bei möglichen Fehlerszenarien

Der erste Punkt ist die Befehlsausgabe.

Melden Sie sich bei der CMX-Befehlszeile an, und führen Sie den Befehl **cmxctl config controller show aus**.

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

Die CMX-MAC-Adresse und der Hash-Schlüssel sind ebenfalls in der Ausgabe enthalten:

Wenn mindestens eine inaktive Ausgabe vorhanden ist, wird eine Checkliste angezeigt:

1. Erreichbarkeit
2. Zeit

3. Simple Network Management Protocol (SNMP) 161-Port
4. NMSP 16113-Port
5. Version
6. Korrekter Hash auf den Controller gedrückt

Überprüfung der Erreichbarkeit

Um die Verfügbarkeit für den Controller zu überprüfen, führen Sie einen Ping von CMX zum WLC aus.

Zeitsynchronisierung

Die Best Practice besteht darin, sowohl CMX als auch WLC auf denselben NTP-Server (Network Time Protocol) zu verweisen.

In Unified WLC (AireOS) wird dies mit dem folgenden Befehl festgelegt:

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

Führen Sie in IOS-XE für den konvergenten Zugriff den folgenden Befehl aus:

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

So ändern Sie die IP-Adresse des NTP-Servers in CMX (vor CMX 10.6):

Schritt 1: Melden Sie sich bei der Befehlszeile als **cmxadmin** an, wechseln Sie zu root user **<su root>**.

Schritt 2: Beenden Sie alle CMX-Dienste mit dem Befehl **cmxctl stop -a**.

Schritt 3: Beenden Sie den NTP-Daemon mit dem Befehl **service ntpd stop**.

Schritt 4: Wenn alle Prozesse beendet sind, führen Sie den Befehl **über /etc/ntp.conf aus**. Klicken Sie auf **i**, um in den Einfügemodus zu wechseln und die IP-Adresse zu ändern. Klicken Sie anschließend auf **ESC**, und geben Sie **:wq** ein, um die Konfiguration zu speichern.

Schritt 5: Nach der Parameteränderung starten Sie den Befehl **service ntpd start**.

Schritt 6: Überprüfen Sie, ob der NTP-Server mit dem Befehl **ntpdate -d <IP-Adresse des NTP-Servers>** erreichbar ist.

Schritt 7: Warten Sie mindestens fünf Minuten, bis der NTP-Dienst neu gestartet und mit dem Befehl **ntpstat** verifiziert wird.

Schritt 8: Nachdem der NTP-Server mit CMX synchronisiert wurde, führen Sie den Befehl **cmxctl restart aus**, um die CMX-Dienste neu zu starten, und wechseln Sie zurück zum **cmxadmin-**Benutzer.

Nach CMX 10.6 können Sie die CMX-NTP-Konfiguration wie folgt überprüfen und ändern:

Schritt 1: Melden Sie sich als **cmxadmin** bei der Befehlszeile an.

Schritt 2: Überprüfen Sie die NTP-Synchronisierung mit **cmxos health ntp.**

Schritt 3: Wenn Sie den NTP-Server neu konfigurieren möchten, können Sie **cmxos ntp clear** und dann den **cmxos ntp-Typ** verwenden.

Schritt 4: Nachdem der NTP-Server mit CMX synchronisiert wurde, führen Sie den Befehl **cmxctl restart aus**, um die CMX-Dienste neu zu starten, und wechseln Sie zurück zum **cmxadmin-**Benutzer.

SNMP-Erreichbarkeit

Führen Sie den Befehl in CMX aus, um zu überprüfen, ob CMX auf SNMP zum WLC zugreifen kann:

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

Bei diesem Befehl wird davon ausgegangen, dass der WLC die Standard-SNMP-Version 2 ausführt. In Version 3 sieht der Befehl wie folgt aus:

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

Wenn SNMP nicht aktiviert ist oder der Community-Name falsch ist, gibt es ein Timeout. Wenn der Vorgang erfolgreich ist, wird der gesamte SNMP-Datenbankinhalt des WLC angezeigt.

> **Hinweis**: Die Verbindung zwischen CMX und WLC wird nicht hergestellt, wenn sich CMX im gleichen Subnetz wie der WLC-Service-Port befindet.

NMSP-Erreichbarkeit

Führen Sie die folgenden Befehle aus, um zu überprüfen, ob CMX auf NMSP zum WLC zugreifen kann:

In CMX:

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

Im WLC:

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

Versionskompatibilität

Überprüfen Sie die Kompatibilität der Version mit dem neuesten Dokument.

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

Korrekter Hash auf Controller gedrückt

Hash auf Controller-seitigem AireOS nicht vorhanden

Normalerweise fügt der wlc automatisch die sha2 und den Benutzernamen hinzu. Die Schlüssel können mit dem Befehl **show auth-list** überprüft werden.

```
(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
```

Wenn der Hashschlüssel und die MAC-Adresse von CMX in der Tabelle nicht vorhanden sind, können Sie in WLC manuell hinzufügen:

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

Hash ist auf Controller-seitigem konvergentem Zugriff IOS-XE nicht vorhanden

Bei NGWC-Controllern müssen die Befehle wie folgt manuell ausgeführt werden:

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

Hinweis: cmx mac-addr muss ohne Satzzeichen-Doppelpunkt (:) hinzugefügt werden.

So beheben Sie die Hash-Taste:

```
 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
```

Falls weiterhin Probleme auftreten, besuchen Sie die Cisco Support-Foren, um Hilfe zu erhalten. Die in diesem Artikel erwähnten Ausgaben und Checklisten können Ihnen definitiv helfen, Ihr Problem in den Foren einzugrenzen oder eine TAC Support Anfrage zu öffnen.