WLC로 CMX 연결 문제 해결

목차

소개

이 문서에서는 CMX(Unified 및 Converged with Connected Mobile Experience)와 같은 WLC(Wireless LAN Controller)의 연결 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco는 구성 프로세스 및 구축 가이드에 대한 지식을 보유하고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CMX 10.2.3-34
- WLC 2504 / 8.2.141.0
- 가상 WLC 8.3.102.0
- 통합 액세스 WLC C3650-24TS / 03.06.05E

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

참고:CMX 10.6을 사용하는 경우 루트 사용자로 전환하려면 특수 패치가 설치되어 있어야 합니다 .Cisco TAC에 문의하여 설치를 요청하십시오.

또한 루트 패치가 있더라도 전체 경로(예:"/bin/snmpwalk.." "snmpwalk"가 작동하지 않을 경우

배경 정보

이 문서에서는 WLC가 CMX에 추가되고 실패하거나 WLC가 유효하지 않거나 비활성 상태로 표시되는 상황에 대해 중점적으로 설명합니다.기본적으로 NMSP(Network Mobility Service Protocol) 터널이 나타나지 않거나 NMSP 통신이 비활성 상태로 표시되는 경우

WLC와 CMX 간의 통신은 NMSP를 사용하여 이루어집니다.

NMSP는 WLC를 향해 TCP 포트 16113에서 실행되고 TLS를 기반으로 실행되며, MSE(Mobility Services Engine)/CMX와 컨트롤러 간 인증서(키 해시) 교환이 필요합니다.WLC와 CMX 간의 TLS/SSL(Transport Layer Security/Secure Sockets Layer) 터널은 컨트롤러에서 시작됩니다.

가능한 장애 시나리오 문제 해결

이 명령 출력으로 첫 번째로 시작할 수 있습니다.

CMX 명령줄에 로그인하고 명령 cmxctl config **controller show를 실행합니다**.

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

또한 CMX MAC 주소와 해시 키는 출력에서 찾을 수 있습니다.

하나 이상의 비활성 상태가 있는 경우 다음과 같은 체크리스트가 표시됩니다.

1. 연결성
2. 시간
3. SNMP(Simple Network Management Protocol) 161 포트
4. NMSP 16113 포트
5. 버전
6. 컨트롤러에서 올바른 해시 푸시됨

연결성 확인

컨트롤러에 연결할 수 있는지 확인하려면 CMX에서 WLC로 ping을 실행합니다.

시간 동기화

모범 사례는 CMX와 WLC를 모두 동일한 NTP(Network Time Protocol) 서버로 지정하는 것입니다.

Unified WLC(AireOS)에서는 다음 명령으로 설정됩니다.

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

통합 액세스 IOS-XE에서 다음 명령을 실행합니다.

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

CMX에서 NTP 서버의 IP 주소를 변경하려면(CMX 10.6 이전)

1단계. 명령줄에 cmxadmin으로 **로그인하고** 루트 사용자 **<su root>**로 전환합니다.

2단계. cmxctl stop -a 명령을 사용하여 모든 CMX 서비스**를 중지합니다**.

3단계. 명령 **서비스 ntpd stop**을 사용하여 NTP **데몬을 중지합니다**.

4단계. 모든 프로세스가 중지되면 /etc/ntp.conf **vi** 명령을 실행합니다. **i를** 클릭하여 삽입 모드로 전환하고 IP 주소를 변경한 다음 **ESC**를 클릭하고 **:wq를 입력하여** 구성을 저장합니다.

5단계. 매개변수가 변경되면 명령 **서비스 ntpd 시작**을 **실행합니다**.

6단계. NTP 서버가 ntpdate -**d <IP address of NTP server>** 명령으로 연결 가능한지 **확인합니다**.

7단계. NTP 서비스를 다시 시작하고 ntpstat 명령을 사용하여 확인하려면 최소 5분 정도 **기다립니다**.

8단계. NTP 서버가 CMX와 동기화되면 cmxctl restart 명령을 실행하여 CMX 서비스를 다시 시작하고 cmxadmin 사용자로 다시 **전환합니다**.

CMX 10.6 이후에는 다음과 같이 CMX NTP 컨피그레이션을 확인하고 변경할 수 있습니다.

1단계. 명령줄에 cmxadmin으로 **로그인합니다.**

2단계. NTP 동기화(cmxos **health ntp)를 확인합니다.**

3단계. NTP 서버를 재구성하려면 cmxos ntp clear를 사용한 다음 **cmxos ntp 유형**을 사용할 수 있습니다.

4단계. NTP 서버가 CMX와 동기화되면 cmxctl restart 명령을 실행하여 CMX 서비스를 다시 시작하고 cmxadmin 사용자로 다시 **전환합니다**.

SNMP 연결성

CMX에서 WLC에 대한 SNMP에 액세스할 수 있는지 확인하려면 CMX에서 명령을 실행합니다.

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

이 명령은 WLC가 기본 SNMP 버전 2를 실행하는 것으로 가정합니다. 버전 3에서는 명령이 다음과 같습니다.

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

SNMP가 활성화되지 않았거나 커뮤니티 이름이 잘못된 경우 시간 초과가 있습니다.성공하면 WLC의 전체 SNMP 데이터베이스 콘텐츠가 표시됩니다.

> **참고:**CMX가 WLC 서비스 포트와 동일한 서브넷에 있는 경우 CMX와 WLC 간의 연결이 설정되지 않습니다.

NMSP 연결 가능성

CMX에서 WLC에 대한 NMSP에 액세스할 수 있는지 확인하려면 다음 명령을 실행합니다.

CMX에서:

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

WLC에서 다음을 수행합니다.

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

버전 호환성

최신 문서와 버전 호환성을 확인합니다.

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

컨트롤러에서 올바른 해시 푸시됨

컨트롤러 측 AireOS에 해시가 없습니다.

일반적으로 wlc는 sha2 및 사용자 이름을 자동으로 추가합니다.키는 show auth-**list** 명령으로 확인할 수 있습니다.

```
(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
```

CMX의 해시 키와 MAC 주소가 테이블에 없는 경우 WLC에서 수동으로 추가할 수 있습니다.

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

컨트롤러 측 통합 액세스 IOS-XE에 해시가 없습니다.

NGWC 컨트롤러에서 다음과 같이 명령을 수동으로 실행해야 합니다.

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

참고:cmx mac-addr은 구두점 마크 콜론(:) 없이 추가해야 합니다.

해시 키를 트러블슈팅하려면

```
 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
```

여전히 문제가 발생하면 cisco support 포럼에서 도움을 요청하십시오.이 문서에서 언급된 결과 및 체크리스트를 통해 포럼에서 문제를 해결하거나 TAC 지원 요청을 열 수 있습니다.