Connectiviteit met probleemoplossing met WLC

Inhoud

Inleiding

Dit document beschrijft de methoden om problemen op te lossen met de connectiviteit van Wireless LAN Controller (WLC), zowel Unified als geconvergeerde met Connected Mobile Experience (CMX).

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van het configuratieproces en de implementatiegids.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CMX 10.2.3-34
- WLC 2504 / 8.2.141.0
- virtuele WLC 8.3.102.0
- geconvergeerde access WLC3650-24TS/03.06.05E

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Opmerking: als u CMX 10.6 gebruikt, moet er een speciaal pleister worden geïnstalleerd om op de

basisgebruiker over te schakelen. Neem contact op met Cisco TAC om dit te laten installeren.

Ook moet u in bepaalde gevallen, zelfs met een wortelpatroon, de opdracht uitvoeren via het volledige pad, bijvoorbeeld. "/trommeltrommel/tussenpoos ..." voor het geval dat " tussenstappen " niet werkt .

Achtergrondinformatie

Dit artikel concentreert zich op situaties waar een WLC aan CMX wordt toegevoegd en het mislukt, of de WLC verschijnt als ongeldig of inactief. Basilicum wanneer de NMSP-tunnel (Network Mobility Service Protocol) niet omhoog komt of de NMSP-communicatie als Inactief verschijnt.

De communicatie tussen de WLC en CMX gebeurt met het gebruik van NMSP.

NMSP loopt op TCP poort 16113 naar de WLC en op TLS gebaseerd, wat een certificaat (key hash) uitwisseling vereist tussen Mobility Services Engine (MSE)/CMX en de controller. De Transport Layer Security/Secure Socket Layer (TLS/SSL)-tunnel tussen de WLC en CMX wordt gestart door de controller.

Probleemoplossing mogelijke mislukkingsscenario's

De eerste te starten plaats is met deze opdrachtoutput.

Meld u aan bij de CMX-opdrachtregel en voer de opdracht **cmxtl-configuratiescontrollers uit**.

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

U kunt ook het CMX-adres en de Hash-key van de uitvoer vinden:

De output, wanneer er minstens één inactief is, toont een controlelijst:

1. bereikbaarheid
2. tijd
3. Simple Network Management Protocol (SNMP) 161-poorts
4. NMSP 1613 poort
5. Versie
6. Correcte hash ingedrukt op de controller

Controleer de bereikbaarheid

Om de bereikbaarheid aan de controller te controleren, voert u een ping uit van CMX naar de WLC.

Tijdsynchroniseren

De beste praktijk is om zowel CMX als de WLC aan de zelfde server van het Protocol van de Netwerktijd (NTP) te richten.

In Unified WLC (AireOS) wordt deze ingesteld met de opdracht:

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

In geconvergeerde toegang IOS-XE, voer de opdracht uit:

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

Zo wijzigt u het IP-adres van de NTP-server in CMX (vóór CMX 10.6):

Stap 1. Meld u aan bij de opdrachtregel als **cmxadmin**, schakel vervolgens over op de basisgebruiker **<su root>**.

Stap 2. Stop alle CMX-services met de opdracht **cmxtl-stop -a**.

Stap 3. Stop de NTP-**indicator** met het **NTP-**nummer.

Stap 4. Nadat al het proces is gestopt, voert u de opdracht **vi /etc/ntp.conf** uit. Klik op **i** om over te schakelen naar de invoegmodus en het IP-adres te wijzigen, dan op **ESC** en type **:wq** om de configuratie op te slaan.

Stap 5. Zodra de parameter is gewijzigd, **start** de **opdrachtservice** ntpd.

Stap 6. Controleer of de NTP-server bereikbaar is met de **opdrachtdatum -d <IP-adres van de NTP-server>**.

Stap 7. Laat ten minste vijf minuten staan voor de NTP-service om opnieuw te starten en te controleren met de opdrachtindex **van TTP**.

Stap 8. Zodra de NTP-server gesynchroniseerd is met CMX, voert u de opdracht **cmxctl opnieuw uit** om de CMX-services te hervatten en terug te schakelen naar de **cmxadmin-**gebruiker.

Na CMX 10.6 kunt u de CMX NTP-configuratie op deze manier verifiëren en wijzigen:

Stap 1. Meld u aan bij de opdrachtregel als **cmxadmin**

Stap 2. Controleer de NTP-synchronisatie met **cmxos status ntp**

Stap 3. Als u de NTP-server wilt opnieuw configureren kunt u **cmxos ntp** gebruiken **helder** en vervolgens **cmxos ntp type**.

Stap 4. Zodra de NTP-server gesynchroniseerd is met CMX, voert u de opdracht **cmxctl opnieuw**

uit om de CMX-services te hervatten en terug te schakelen naar de **cmxadmin-**gebruiker.

SNMP-bereikbaarheid

Om te controleren of CMX toegang heeft tot SNMP in de WLC voert u de opdracht in CMX uit:

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

Deze opdracht is er vanuit gegaan dat WLC de standaard SNMP versie 2 uitvoert. In versie 3 ziet de opdracht er zo uit:

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

Als SNMP niet is ingeschakeld of de naam van de gemeenschap verkeerd is, is er een tijdelijke oplossing. Als het succesvol is, ziet u de volledige inhoud van de SNMP-database van de WLC.

> Opmerking: De verbinding tussen CMX en WLC zal niet worden gevestigd als CMX in zelfde Subnet zoals de diensthaven van WLC is.

NMSP-bereikbaarheid

Om te controleren of CMX toegang heeft tot NMSP in de WLC voert u de opdrachten uit:

In CMX:

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

In de WLC:

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

Compatibiliteit met versie

Controleer de compatibiliteit van de versie met het nieuwste document.

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

Hash ingedrukt op controller

Hash niet aanwezig op Controller Side Aire OS

Gewoonlijk voegt de wlc automatisch sha2 en de gebruikersnaam toe. De toetsen kunnen worden geverifieerd met de opdracht **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
```

Als de hash key en het MAC adres van CMX niet in tabel aanwezig zijn, dan is het mogelijk om handmatig toe te voegen in WLC:

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

Hash niet aanwezig op Controller zijde geconvergeerde access IOS-XE

In NGWC-controllers moet u de opdrachten als volgt handmatig uitvoeren:

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

> Opmerking: cmx mac-addr moet worden toegevoegd zonder punctutieteken colon (:)

Zo lost u de hash-toets op:

```
 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
```

Als u nog steeds problemen ondervindt, bezoek dan Cisco-ondersteuningsforums voor hulp. De resultaten en controlelijst die in dit artikel worden genoemd kunnen u zeker helpen uw probleem op de forums te beperken of u kunt een TAC ondersteuningsverzoek openen.