Risoluzione dei problemi di connettività CMX con WLC

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Risoluzione dei problemi relativi a possibili scenari di errore](#)
[Verifica della raggiungibilità](#)
[Sincronizzazione ora](#)
[Raggiungibilità SNMP](#)
[Raggiungibilità dell'NMSP](#)
[Compatibilità delle versioni](#)
[Hash corretto applicato al controller](#)
[Hash non presente sull'AireOS lato controller](#)
[Hash non presente sull'accesso convergente lato controller IOS-XE](#)

Introduzione

In questo documento vengono descritti i metodi per risolvere i problemi di connettività del controller WLC (Wireless LAN Controller), sia unificato che convergente con Connected Mobile Experience (CMX).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza del processo di configurazione e della guida all'installazione.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Nota: se si utilizza CMX 10.6, per passare all'utente root è necessario che sia installata una patch speciale. Per installarlo, contattare Cisco TAC.

Inoltre, in alcuni casi anche con una patch di root è necessario eseguire il comando utilizzando il percorso completo, ad esempio "/bin/snmpwalk ..." nel caso "snmpwalk" non funzioni.

Premesse

In questo articolo vengono descritte le situazioni in cui un WLC viene aggiunto al CMX e si guasta oppure viene visualizzato come non valido o non attivo. In pratica, quando il tunnel NMSP (Network Mobility Service Protocol) non viene visualizzato o le comunicazioni NMSP vengono visualizzate come Inattive.

La comunicazione tra WLC e CMX avviene con l'uso di NMSP.

L'NMSP viene eseguito sulla porta TCP 16113 verso il WLC e basato su TLS, che richiede uno scambio di certificati (hash chiave) tra Mobility Services Engine (MSE)/CMX e il controller. Il tunnel Transport Layer Security/Secure Sockets Layer (TLS/SSL) tra WLC e CMX viene avviato dal controller.

Risoluzione dei problemi relativi a possibili scenari di errore

La prima posizione da cui iniziare è con questo output del comando.

Accedere alla riga di comando CMX ed eseguire il comando **cmxctl config controller 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         |
+------------------+--------------------------------------------------------------------------+
```

Inoltre, l'indirizzo MAC CMX e la chiave hash sono disponibili nell'output:

L'output, quando ne è presente almeno uno inattivo, mostra un elenco di controllo:

1. Raggiungibilità
2. Ora
3. Porta SNMP (Simple Network Management Protocol) 161
4. Porta NMSP 1613

5. Version
6. Hash corretto applicato al controller

Verifica della raggiungibilità

Per verificare la raggiungibilità del controller, eseguire un ping tra CMX e WLC.

Sincronizzazione ora

La procedura ottimale consiste nel puntare sia CMX che WLC allo stesso server Network Time Protocol (NTP).

In Unified WLC (AireOS), questa impostazione viene effettuata con il comando:

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

In CNA IOS-XE, eseguire il comando:

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

Per modificare l'indirizzo IP del server NTP in CMX (prima di CMX 10.6):

Passaggio 1. Accedere alla riga di comando come **cmxadmin**, passare all'utente root **<su root>**.

Passaggio 2. Arrestare tutti i servizi CMX con il comando **cmxctl stop -a**.

Passaggio 3. Arrestare il deamon NTP con il comando **service ntpd stop**.

Passaggio 4. Una volta interrotto il processo, eseguire il comando **tramite /etc/ntp.conf**. Fare clic su **i** per passare alla modalità di inserimento e modificare l'indirizzo IP, quindi fare clic su **ESC** e digitare **:wq** per salvare la configurazione.

Passaggio 5. Dopo aver modificato il parametro, eseguire il comando **service ntpd start**.

Passaggio 6. Verificare se il server NTP è raggiungibile con il comando **ntpdate -d <indirizzo IP del server NTP>**.

Passaggio 7. Attendere almeno cinque minuti prima che il servizio NTP venga riavviato e verificato con il comando **ntpstat**.

Passaggio 8. Dopo aver sincronizzato il server NTP con CMX, eseguire il comando **cmxctl restart** per riavviare i servizi CMX e tornare all'utente **cmxadmin**.

Dopo CMX 10.6, è possibile verificare e modificare la configurazione CMX NTP nel modo seguente:

Passaggio 1. Accedere alla riga di comando come **cmxadmin**

Passaggio 2. Controllare la sincronizzazione NTP con **ntp integrità cmxos**

Passaggio 3. Se si desidera riconfigurare il server NTP, è possibile utilizzare **cmxos ntp clear** e quindi **cmxos ntp type**.

Passaggio 4. Dopo aver sincronizzato il server NTP con CMX, eseguire il comando **cmxctl restart** per riavviare i servizi CMX e tornare all'utente **cmxadmin**.

Raggiungibilità SNMP

Per verificare se CMX può accedere al protocollo SNMP sul WLC, eseguire il comando in CMX:

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

Questo comando presuppone che il WLC esegua il protocollo SNMP versione 2 predefinito. Nella versione 3, il comando ha il seguente aspetto:

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

Se il protocollo SNMP non è abilitato o il nome della community è errato, si verifica un timeout. Se l'operazione ha esito positivo, sarà possibile visualizzare l'intero contenuto del database SNMP del WLC.

> **Nota:** La connessione tra CMX e WLC non verrà stabilita se CMX si trova nella stessa subnet della porta del servizio WLC.

Raggiungibilità dell'NMSP

Per verificare se CMX può accedere a NMSP sul WLC, eseguire i comandi:

In CMX:

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

Nel WLC:

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

Compatibilità delle versioni

Verificare la compatibilità della versione con il documento più recente.

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

Hash corretto applicato al controller

Hash non presente sull'AireOS lato controller

In genere, il wlc aggiunge automaticamente sha2 e il nome utente. Le chiavi possono essere verificate con il comando **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
```

Se la chiave hash e l'indirizzo MAC di CMX non sono presenti nella tabella, è possibile aggiungerli manualmente in WLC:

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

Hash non presente sull'accesso convergente lato controller IOS-XE

Nei controller NGWC, è necessario eseguire i comandi manualmente come indicato di seguito:

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

Nota: cmx mac-addr deve essere aggiunto senza segni di punteggiatura due punti (:)

Per risolvere i problemi relativi alla chiave hash:

```
 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
```

Se il problema persiste, visita i forum di assistenza cisco per ottenere assistenza. I risultati e l'elenco di controllo menzionati in questo articolo possono aiutarti a risolvere il problema nei forum o puoi aprire una richiesta di assistenza TAC.