Resolución de Problemas de Conectividad CMX con WLC

Contenido

Introducción

Este documento describe los métodos para solucionar los problemas de conectividad del controlador de LAN inalámbrica (WLC), tanto de Unified como convergente con Connected Mobile Experience (CMX).

Prerequisites

Requirements

Cisco recomienda que conozca el proceso de configuración y la guía de implementación.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CMX 10.2.3-34
- WLC 2504 / 8.2.141.0
- WLC virtual 8.3.102.0
- WLC C3650-24TS / 03.06.05E de acceso convergente

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Nota: si utiliza CMX 10.6, necesita tener instalado un parche especial para cambiar al usuario root. Póngase en contacto con el TAC de Cisco para instalarlo.

Además, en algunos casos, incluso con un parche raíz, necesita ejecutar el comando usando la ruta completa, por ejemplo, "/bin/snmpwalk ..." en caso de que "snmpwalk" no funcione.

Antecedentes

Este artículo se centra en situaciones donde un WLC se agrega al CMX y falla, o el WLC aparece como inválido o inactivo. Básicamente, cuando el túnel del protocolo de servicio de movilidad de red (NMSP) no se activa o las comunicaciones de NMSP aparecen como Inactivas.

La comunicación entre el WLC y el CMX ocurre con el uso de NMSP.

NMSP se ejecuta en el puerto TCP 16113 hacia el WLC y basado en TLS, que requiere un intercambio de certificado (hash de clave) entre Mobility Services Engine (MSE)/CMX y el controlador. El túnel de seguridad de la capa de transporte/capa de sockets seguros (TLS/SSL) entre el WLC y el CMX es iniciado por el controlador.

Solución de posibles escenarios de fallos

El primer lugar para comenzar es con este resultado de comando.

Inicie sesión en la línea de comandos CMX y ejecute el comando **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         |
+------------------+--------------------------------------------------------------------------+
```

Además, la dirección MAC de CMX y la tecla hash se pueden encontrar en la salida:

El resultado, cuando hay al menos un inactivo, muestra una lista de verificación:

1. Alcance
2. Hora
3. Puerto SNMP (protocolo simple de administración de red) 161
4. Puerto NMSP 16113
5. Versión
6. Hash correcto presionado en el controlador

Verificar disponibilidad

Para verificar el alcance al controlador, ejecute un ping de CMX al WLC.

Sincronización horaria

La mejor práctica es señalar tanto CMX como el WLC al mismo servidor de protocolo de tiempo de red (NTP).

En Unified WLC (AireOS), esto se establece con el comando:

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

En el acceso convergente de IOS-XE, ejecute el comando:

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

Para cambiar la dirección IP del servidor NTP en CMX (antes de CMX 10.6):

Paso 1. Inicie sesión en la línea de comandos como **cmxadmin**, cambie al usuario raíz **<su root>**.

Paso 2. Detenga todos los servicios CMX con el comando **cmxctl stop -a**.

Paso 3. Detenga el deamon NTP con el comando **service ntpd stop**.

Paso 4. Una vez que se haya detenido todo el proceso, ejecute el comando **vi /etc/ntp.conf**. Haga clic en **i** para cambiar al modo de inserción y cambiar la dirección IP, luego haga clic en **ESC** y escriba **:wq** para guardar la configuración.

Paso 5. Una vez que se cambia el parámetro, ejecute el comando **service ntpd start**.

Paso 6. Verifique si el servidor NTP es accesible con el comando **ntpdate -d <dirección IP del servidor NTP>** .

Paso 7. Permita al menos cinco minutos para que el servicio NTP se reinicie y verifique con el comando **ntpstat**.

Paso 8. Una vez que el servidor NTP se sincroniza con CMX, ejecute el comando **cmxctl restart** para reiniciar los servicios CMX y volver al usuario **cmxadmin**.

Después de CMX 10.6, puede verificar y cambiar la configuración CMX NTP de esta manera :

Paso 1. Inicie sesión en la línea de comandos como **cmxadmin**

Paso 2. Verifique la sincronización NTP con **cmxos health ntp**

Paso 3. Si desea reconfigurar el servidor NTP, puede utilizar **cmxos ntp clear** y luego **cmxos ntp type**.

Paso 4. Una vez que el servidor NTP se sincroniza con CMX, ejecute el comando **cmxctl restart** para reiniciar los servicios CMX y volver al usuario **cmxadmin**.

Alcance de SNMP

Para verificar si CMX puede acceder a SNMP al WLC, ejecute el comando en CMX:

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

Este comando asume que el WLC ejecuta la versión 2 SNMP predeterminada. En la versión 3, el comando es similar a :

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

Si SNMP no está habilitado o el nombre de la comunidad es incorrecto, se agotará el tiempo de espera. Si es exitoso, verá todo el contenido de la base de datos SNMP del WLC.

> **Nota:** La conexión entre CMX y WLC no se establecerá si CMX está en la misma subred que el puerto de servicio WLC.

Disponibilidad de NMSP

Para verificar si CMX puede acceder a NMSP al WLC, ejecute los comandos:

En CMX:

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

En el WLC:

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

Compatibilidad de versiones

Compruebe la compatibilidad de la versión con el documento más reciente.

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

Hash correcto presionado en el controlador

Hash no está presente en el AireOS del lado del controlador

Normalmente, el wlc agrega automáticamente el sha2 y el nombre de usuario. Las claves se pueden verificar con el 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
```

Si la llave hash y la dirección MAC de CMX no están presentes en la tabla, entonces es posible agregar manualmente en el WLC:

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

Hash no está presente en el acceso convergente del lado del controlador IOS-XE

En los controladores NGWC, debe ejecutar manualmente los comandos de la siguiente manera:

```
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 se debe agregar sin signo de puntuación dos puntos (:)

Para resolver problemas de la llave 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
```

Si todavía tiene problemas, visite foros de soporte de cisco para obtener ayuda. Los resultados y la lista de comprobación mencionados en este artículo pueden ayudarle definitivamente a reducir su problema en los foros o puede abrir una solicitud de soporte del TAC.