Resolver problemas la Conectividad CMX con el WLC

Contenido

Introducción

Este documento describe los métodos para resolver problemas los problemas de conectividad del regulador del Wireless LAN (WLC), unificado y convergido con la experiencia móvil conectada (CMX).

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento del proceso de configuración y del Guía de despliegue.

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 convergido C3650-24TS/03.06.05E del acceso

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Antecedentes

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

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

NMSP se ejecuta en el puerto TCP 16113 hacia el WLC y basados en TLS, que requiere un intercambio del certificado (hash dominante) entre el motor de los Servicios de movilidad (MSE) /CMX y el regulador. El túnel de Transport Layer Security/de Secure Sockets Layer (TLS/SSL) entre el WLC y CMX es iniciado por el regulador.

Resolver problemas los escenarios de la falla posible

El primer lugar a comenzar está con esta salida de comando.

El registro en la línea de comando CMX y ejecutado los **reguladores de los config del cmxctl del** comando **muestra**.

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

También, la dirección MAC CMX y la Hash-clave se pueden encontrar de la salida:

La salida, cuando hay por lo menos una inactiva, muestra una lista de verificación:

1. Alcance
2. Hora
3. Puerto del Simple Network Management Protocol (SNMP) 161
4. Puerto NMSP 16113
5. Versión
6. Hash correcto avanzado en el regulador

Verifique el accesibilidad

Para marcar el accesibilidad al regulador, funcione con un ping a partir de CMX al WLC.

Sincronización horaria

La mejor práctica es señalar ambo CMX y el WLC al mismo servidor del Network Time Protocol (NTP).

En el WLC unificado (AireOS), esto se fija con el comando:

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

En el acceso convergido IOS-XE, funcione con el comando:

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

Para cambiar la dirección IP del servidor NTP en CMX:

Paso 1. Registro en la línea de comando como **cmxadmin**, Switch al **root> del <**su del usuario raíz.

Paso 2. Pare todos los servicios CMX con la **parada del cmxctl del** comando **- a**.

Paso 3. Pare el deamon NTP con la **parada del ntpd del** comando service.

Paso 4. Una vez que se para todo el proceso, funcione con el comando vi **/etc/ntp.conf**. Haga clic **i** para conmutar al modo de inserción y para cambiar la dirección IP, después para hacer clic el **ESC** y para teclear**: wq** para salvar la configuración.

Paso 5. Una vez que se cambia el parámetro ejecute el **comienzo del ntpd del** comando service.

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

Paso 7. Permita que cinco minutos por lo menos, porque el servicio NTP recomiencen y verifiquen con el **ntpstat del** comando.

Paso 8. Una vez que sincronizan al servidor NTP con CMX, ejecute el **reinicio del cmxctl del** comando para recomenzar los servicios CMX y el Switch de nuevo al usuario del **cmxadmin**.

Accesibilidad SNMP

Para marcar si CMX puede acceder el SNMP al WLC, funcione con el comando en CMX:

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

Este comando asume que el WLC funciona con la versión de SNMP predeterminada 2. En la versión 3, el comando parece:

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

Si el SNMP no se habilita, o el nombre de la comunidad es mal allí es un descanso. Si es acertado, usted ve el contenido entero de la base de datos SNMP del WLC.

Accesibilidad NMSP

Para marcar si CMX puede acceder NMSP al WLC, funcione con los comandos:

En CMX:

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

En el WLC:

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

Compatibilidad de versión

Marque la Compatibilidad de versión con el último documento.

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

Hash correcto avanzado en el regulador

Hash no presente en el lado AireOS del regulador

Generalmente, el wlc agrega automáticamente el sha2 y el nombre de usuario. Las claves se pueden verificar con la auténtico-**lista del** comando show.

```
(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 clave del hash y la dirección MAC de CMX no están presentes en la tabla, después es posible agregar manualmente en el WLC:

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

El hash no presente en el lado del regulador convergió el acceso IOS-XE

En los reguladores NGWC, usted necesita funcionar con los comandos manualmente como sigue:

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

> **Note**: las direcciones MAC cmx deben ser agregadas sin los dos puntos del signo de puntuación (:)

Para resolver problemas la clave del 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 usted todavía hace frente a cualesquiera problemas, visite los foros del soporte de Cisco para la ayuda. Las salidas y la lista de verificación mencionadas en este artículo pueden ayudarle definitivamente a estrechar abajo su problema en los foros o usted puede abrir una petición del soporte a TAC.