Resolver problemas la Conectividad CMX con el WLC

Contenido

Introducción

Este documento analiza los métodos para resolver problemas los problemas de conectividad del regulador del Wireless LAN (WLC): unificado y convergido con la experiencia móvil conectada (CMX). Se centra en las situaciones donde agregar un WLC al CMX falla o el WLC aparece como inválido o inactivo: básicamente cuando no sube el túnel NMSP (Protocolo de servicio de la movilidad de la red).

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 MSE/CMX y el regulador. El túnel TLS/SSL entre el WLC y CMX es iniciado por el regulador.

Prerrequisitos

Componentes usados

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

Requisitos

Este documento asume que usted es ya familiar con el proceso de configuración y el Guía de despliegue. Se centra solamente en las situaciones de Troubleshooting en donde las comunicaciones NMSP aparecen como inactivo

Resolución de problemas: escenarios de la falla posible

El primer lugar a comenzar es el siguiente comando hecho salir:

Inicie sesión en la línea de comando CMX y funcione con el comando “demostración de los reguladores de los config del cmxctl”

```
** 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, de la salida usted puede descubrir la dirección MAC CMX y la Hash-clave:

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

1. Alcance
2. Hora
3. Puerto SNMP 161
4. Puerto NMSP 16113
5. Versión
6. Hash correcto avanzado en el regulador

1- Verifique el accesibilidad

Para marcar el accesibilidad al regulador publique un ping a partir de CMX al WLC

sincronización 2-Time

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:

```
(config)#ntp server <IP address of NTP>
```
Para cambiar la dirección IP del servidor NTP en CMX:

1. Login a la línea de comando como cmxadmin, Switch al root> del <su del usuario raíz
2. Pare todos los servicios con el comando “parada del cmxctl -”
3. Una vez que se para todo el proceso, ingrese el comando “VI /etc/ntp.conf”: presióneme “” conmutar al modo de inserción y cambiar la dirección IP, después para presionar el “ESC” y para teclear “: wq” para salvar la configuración;
4. Una vez que se cambia el parámetro, publique el comando “reinicio del cmxctl” de recomenzar los servicios y el Switch de nuevo al usuario del cmxadmin.

Accesibilidad 3-SNMP

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

```
Snmpwalk -c <name of community> -v 2c <IP address of WLC>.
```
El comando antedicho asume que el WLC funciona con la versión de SNMP predeterminada 2. en caso de que usted utilice la versión 3 solamente, el comando parecería:

```
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 incorrecto allí será un descanso. Si es acertado, usted verá el contenido entero de la base de datos SNMP del WLC.

Accesibilidad 4-NMSP

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

En CMX:

```
 netstat -a | grep 16113
```
En el WLC:

```
show nmsp status
show nmsp subscription summary
```
compatibilidad 5-Version

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 6-Correct avanzado en el regulador

6a) Hash no presente en el lado AireOS del regulador

Generalmente, el wlc agrega automáticamente el sha2 y el nombre de usuario y las claves se pueden verificar con el comando: muestre la auténtico-lista

```
(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 el MAC address 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>
```

6b) **El hash no presente en el lado del regulador convergió el acceso IOS-XE**

En el regulador 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 >
```

Nota: las direcciones MAC cmx deben ser agregadas sin la columna (:)

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
```

¿Todavía tener problemas?

¡Si todos los antedichos no señalan al problema, no dude en visitar los foros del soporte de Cisco para la ayuda (las salidas y la lista de verificación antedichas ayudarán definitivamente a estrechar abajo su problema en los foros) o a abrir una petición del soporte a TAC!