Dépannage de la Connectivité CMX avec WLC

Contenu

Introduction

Ce document analyse les méthodes pour dépanner les problèmes de connectivité du contrôleur LAN Sans fil (WLC) : unifié et convergé avec l'expérience de la mobilité connectée (CMX). Il se concentre sur des situations où ajoutant un WLC au CMX échoue ou le WLC apparaît comme non valide ou inactif : fondamentalement quand le tunnel NMSP (service Protocol de mobilité de réseau) ne monte pas.

La transmission entre le WLC et CMX se produit avec l'utilisation de NMSP.

NMSP fonctionne sur le port TCP 16113 vers le WLC et basés sur le TLS, qui exige un échange de certificat (informations parasites principales) entre MSE/CMX et le contrôleur. Le tunnel TLS/SSL entre le WLC et CMX est initié par le contrôleur.

Conditions préalables

Composants utilisés

CMX 10.2.3-34

WLC 2504/8.2.141.0

WLC virtuel 8.3.102.0

Access convergé WLC C3650-24TS/03.06.05E

Conditions requises

Ce document suppose que vous êtes déjà au courant du processus de configuration et du guide

de déploiement. Il se concentre seulement sur des situations de dépannage où les transmissions NMSP apparaissent comme inactif

Dépannage : scénarios de panne possibles

Le premier endroit à commencer est la sortie de commande suivante :

Ouvrez une session dans la ligne de la commande CMX et exécutez la commande « exposition de contrôleurs de config de 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        |
+------------------+-------------------------------------------------------------------------+
```

En outre, de la sortie vous pouvez découvrir l'adresse MAC CMX et l'Information-clé :

La sortie, quand il y a au moins d'une inactive, affichera une liste de contrôle :

1. Accessibilité
2. Heure
3. Port SNMP 161
4. Port NMSP 16113
5. Version
6. Informations parasites correctes poussées sur le contrôleur

1- Vérifiez l'accessibilité

Pour vérifier l'accessibilité au contrôleur fournissez un ping de CMX au WLC

synchronisation 2-Time

La pratique recommandée est d'indiquer les deux CMX et le WLC le même serveur de Protocole NTP (Network Time Protocol).

Dans WLC unifié (AireOS) ceci est placé avec la commande :

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

Dans l'accès convergé IOS-XE :

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

Pour changer l'adresse IP du serveur de NTP dans CMX :

1. Procédure de connexion à la ligne de commande comme cmxadmin, commutateur au root> de <su d'utilisateur de base
2. Arrêtez tous les services avec la commande « arrêt de cmxctl - »
3. Une fois que tout le processus sont arrêtés, sélectionnez la commande « vi /etc/ntp.conf » : appuyez sur-« moi » pour commuter au mode d'insertion et pour changer l'adresse IP, puis pour appuyer sur le « ESC » et pour taper « : wq » pour sauvegarder la configuration ;
4. Une fois que le paramètre est changé, émettez la commande « reprise de cmxctl » de redémarrer les services et de commuter de nouveau à l'utilisateur de cmxadmin.

Accessibilité 3-SNMP

Pour vérifier si CMX peut accéder au SNMP au WLC, émettez la commande dans CMX :

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

La commande ci-dessus suppose que le WLC exécute la version 2. SNMP de par défaut au cas où vous utiliseriez la version 3 seulement, la commande ressemblerait à :

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

Si le SNMP n'est pas activé, ou le nom de communauté est erroné là sera un délai d'attente. Si réussi, vous verrez la teneur entière en base de données SNMP du WLC.

Accessibilité 4-NMSP

Pour vérifier si CMX peut accéder à NMSP au WLC, émettez les commandes :

Dans CMX :

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

Dans le WLC :

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

compatibilité 5-Version

Vérifiez la compatibilité de version avec le dernier document.

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

informations parasites 6-Correct poussées sur le contrôleur

6a) Hachez non actuel du côté AireOS de contrôleur

Habituellement, le wlc ajoutent automatiquement le sha2 et le nom d'utilisateur et les clés peuvent être vérifiées avec la commande : 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 clé d'informations parasites et le MAC address de CMX ne sont pas présents dans la table, alors il est possible d'ajouter manuellement dans WLC :

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

6b) **Les informations parasites non actuelles du côté de contrôleur ont convergé l'accès IOS-XE**

Dans le contrôleur NGWC vous devez exécuter les commandes manuellement comme suit :

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

Remarque: le MAC-adr cmx devrait être ajouté sans colonne (:)

Pour dépanner la clé d'informations parasites :

```
 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
```

Avoir toujours des problèmes ?

Si tous les ci-dessus n'indiquent pas le problème, se sentir libres de visiter des forum de support de Cisco pour l'aide (les sorties et la liste de contrôle ci-dessus aideront certainement à rétrécir vers le bas votre problème sur les forum) ou à ouvrir une demande de support TAC !