Dépannage de la Connectivité CMX avec WLC

Contenu

Introduction

Ce document décrit 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).

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance du processus de configuration et du guide de déploiement.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Informations générales

Cet article se concentre sur des situations où un WLC est ajouté au CMX et il échoue, ou le WLC apparaît comme non valide ou inactif. Fondamentalement quand le tunnel de Protocol de service de mobilité de réseau (NMSP) ne monte pas ou les transmissions NMSP révèle comme inactif.

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 l'engine de Services de mobilité (MSE) /CMX et le contrôleur. Le tunnel de Transport Layer Security/Secure Sockets Layer (TLS/SSL) entre le WLC et CMX est initié par le contrôleur.

Dépannage des scénarios de panne possibles

Le premier endroit à commencer est avec cette sortie de commande.

Connectez-vous dans la ligne de la commande CMX et exécutez l'**exposition de contrôleurs de config de cmxctl de** commande.

```
** 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, l'adresse MAC CMX et l'Information-clé peuvent être trouvées de la sortie :

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

1. Accessibilité
2. Heure
3. Port du Protocole SNMP (Simple Network Management Protocol) 161
4. Port NMSP 16113
5. Version
6. Informations parasites correctes poussées sur le contrôleur

Vérifiez l'accessibilité

Afin de vérifier l'accessibilité au contrôleur, exécutez un ping de CMX au WLC.

Synchronisation temporelle

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, exécutez la commande :

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

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

Étape 1. Connectez-vous dans la ligne de commande comme **cmxadmin**, commutez au **root> de <**su d'utilisateur de base.

Étape 2. Arrêtez tous les services CMX avec l'**arrêt de cmxctl de** commande **- a**.

Étape 3. Arrêtez le deamon de NTP avec l'**arrêt de ntpd de service de** commande.

Étape 4. Une fois que tout le processus sont arrêtés, exécutez la commande **vi /etc/ntp.conf**. Cliquez sur **I** pour commuter au mode d'insertion et pour changer l'adresse IP, puis pour cliquer sur l'**ESC** et pour taper **: wq** pour sauvegarder la configuration.

Étape 5. Une fois que le paramètre est changé exécutez le **début de ntpd de service de** commande.

Étape 6. Vérifiez si le serveur de NTP est accessible avec le **ntpdate de** commande **- d < adresse IP de server> de NTP**.

Étape 7. Permettez à cinq minutes au moins, parce que au service de NTP pour redémarrer et vérifier avec le **ntpstat de** commande.

Étape 8. Une fois que le serveur de NTP est synchronisé avec CMX, exécutez la **reprise de cmxctl de** commande pour redémarrer les services CMX et pour commuter de nouveau à l'utilisateur de **cmxadmin**.

Accessibilité SNMP

Afin de vérifier si CMX peut accéder au SNMP au WLC, exécutez la commande dans CMX :

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

Cette commande suppose que le WLC exécute la version 2 SNMP de par défaut. Dans la version 3, la commande ressemble 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 mal il y a un délai d'attente. S'il est réussi, vous voyez la teneur entière en base de données SNMP du WLC.

Accessibilité NMSP

Afin de vérifier si CMX peut accéder à NMSP au WLC, exécutez les commandes :

Dans CMX :

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

Dans le WLC :

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

Compatibilité de 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 correctes poussées sur le contrôleur

Informations parasites non actuelles du côté AireOS de contrôleur

Habituellement, le wlc ajoute automatiquement le sha2 et le nom d'utilisateur. Les clés peuvent être vérifiées avec le **show auth-list de** commande.

```
(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 l'adresse MAC de CMX ne sont pas présentes dans la table, alors il est possible d'ajouter manuellement dans WLC :

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

Informations parasites non actuelles sur le contrôleur Access convergé par côté IOS-XE

Dans des contrôleurs 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 >
```

Note: le MAC-adr cmx doit être ajouté sans deux points de signe de ponctuation (:)

Afin de 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
```

Si vous faites face toujours à n'importe quelles questions, visitez les forum de support de Cisco pour l'aide. Les sorties et la liste de contrôle mentionnées en cet article peuvent certainement vous aider à rétrécir vers le bas votre problème sur les forum ou vous pouvez ouvrir une demande de support TAC.