# Dépannage de la connectivité CMX avec WLC

## Contenu



## Introduction

Ce document décrit les méthodes de dépannage des problèmes de connectivité du contrôleur de réseau local sans fil (WLC), à la fois unifié et convergé avec Connected Mobile Experience (CMX).

## Conditions préalables

### Conditions requises

Cisco vous recommande de connaître le processus de configuration et le guide de déploiement.

### Components Used

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
- WLC d'accès convergé C3650-24TS / 03.06.05E

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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Note: si vous utilisez CMX 10.6, vous devez avoir installé un correctif spécial pour passer à l'utilisateur racine. Contactez le TAC Cisco pour l'installer.

En outre, dans certains cas, même avec un patch racine, vous devez exécuter la commande en utilisant le chemin complet, par exemple. "/bin/snmpwalk ... » au cas où « snmpwalk » ne fonctionnerait pas.

# Informations générales

Cet article se concentre sur les situations où un WLC est ajouté au CMX et qu'il échoue, ou le WLC apparaît comme non valide ou inactif. En fait, lorsque le tunnel NMSP (Network Mobility Service Protocol) ne s'active pas ou que les communications NMSP apparaissent comme inactives.

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

NMSP s'exécute sur le port TCP 16113 vers le WLC et basé sur TLS, qui nécessite un échange de certificat (hachage de clé) entre MSE (Mobility Services Engine)/CMX et le contrôleur. Le tunnel TLS/SSL (Transport Layer Security/Secure Sockets Layer) entre le WLC et le CMX est initié par le contrôleur.

# Dépanner les scénarios de défaillance possibles

La première place à commencer est avec cette sortie de commande.

Connectez-vous à la ligne de commande CMX et exécutez la commande **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       |
+------------------+------------------------------------------------------------------------+
```

En outre, l'adresse MAC CMX et la clé de hachage se trouvent dans le résultat :

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

1. Accessibilité
2. Heure
3. Port SNMP (Simple Network Management Protocol) 161
4. Port NMSP 16113
5. Version
6. Hachage correct poussé sur le contrôleur

## Vérifier l'accessibilité

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

## Synchronisation temporelle

La meilleure pratique consiste à pointer à la fois CMX et le WLC vers le même serveur NTP (Network Time Protocol).

Dans Unified WLC (AireOS), ceci est défini avec la commande :

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

Dans IOS-XE à accès convergé, exécutez la commande suivante :

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

Afin de modifier l'adresse IP du serveur NTP dans CMX (avant CMX 10.6) :

Étape 1. Connectez-vous à la ligne de commande en tant que **cmxadmin**, passez à l'utilisateur racine **<su root>**.

Étape 2. Arrêtez tous les services CMX à l'aide de la commande **cmxctl stop -a**.

Étape 3. Arrêtez le débogage NTP avec la commande **service ntpd stop**.

Étape 4. Une fois le processus arrêté, exécutez la commande **vi /etc/ntp.conf**. Cliquez sur **i** pour passer en mode insertion et modifier l'adresse IP, puis cliquez sur **ESC** et tapez **:wq** pour enregistrer la configuration.

Étape 5. Une fois le paramètre modifié, exécutez la commande **service ntpd start**.

Étape 6. Vérifiez si le serveur NTP est accessible à l'aide de la commande **ntpdate -d <adresse IP du serveur NTP>**.

Étape 7. Comptez au moins cinq minutes pour que le service NTP redémarre et vérifie avec la commande **ntpstat**.

Étape 8. Une fois le serveur NTP synchronisé avec CMX, exécutez la commande **cmxctl restart** pour redémarrer les services CMX et revenir à l'utilisateur **cmxadmin**.

Après CMX 10.6, vous pouvez vérifier et modifier la configuration NTP de CMX de cette manière :

Étape 1. Connectez-vous à la ligne de commande en tant que **cmxadmin**

Étape 2. Vérifier la synchronisation NTP avec **cmxos health ntp**

Étape 3.  Si vous voulez reconfigurer le serveur NTP, vous pouvez utiliser **cmxos ntp clear** puis **cmxos ntp type**.

Étape 4. Une fois le serveur NTP synchronisé avec CMX, exécutez la commande **cmxctl restart** pour redémarrer les services CMX et revenir à l'utilisateur **cmxadmin**.

## Accessibilité SNMP

Afin de vérifier si CMX peut accéder à 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 SNMP version 2 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 protocole SNMP n'est pas activé ou si le nom de la communauté est incorrect, un délai d'attente s'affiche. S'il réussit, vous voyez le contenu complet de la base de données SNMP du WLC.

> **Note**: La connexion entre CMX et WLC ne sera pas établie si CMX se trouve dans le même sous-réseau que le port de service 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 des versions

Vérifiez la compatibilité de la version avec le dernier document.

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

## Hachage correct poussé sur le contrôleur

### Hachage non présent sur AireOS côté contrôleur

Généralement, le wlc ajoute automatiquement le sha2 et le nom d'utilisateur. Les clés peuvent être vérifiées à l'aide de 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 de hachage et l'adresse MAC de CMX ne sont pas présentes dans la table, il est alors possible d'ajouter manuellement dans le WLC :

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

### Hachage non présent sur IOS-XE d'accès convergent côté contrôleur

Dans les 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**: cmx mac-addr doit être ajouté sans signe de ponctuation deux-points (:)

Afin de dépanner la clé de hachage :

```
 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 rencontrez toujours des problèmes, consultez les forums d'assistance Cisco pour obtenir de l'aide. Les résultats et la liste de contrôle mentionnés dans cet article peuvent vous aider à résoudre votre problème sur les forums ou vous pouvez ouvrir une demande d'assistance TAC.