Устранение проблем подключения CMX с WLC

Содержание

[Введение](#)
[Предварительные условия](#)
[Используемые компоненты](#)
[Требования](#)
[Устранение неисправностей: сценарии возможного сбоя](#)
[1-Проверяют достижимость](#)
[2-разовая синхронизация](#)
[Достижимость с 3 SNMP](#)
[4-NMSP достижимость](#)
[5 совместимостей версий](#)
[6-корректный Хэш спешил контроллер](#)
[Проблемы остались?](#)

Введение

Этот документ анализирует методы для устранения проблем проблем с подключением Контроллера беспроводной локальной сети (WLC): оба Унифицированные и Сходившиеся со Связанным Мобильным опытом (CMX). Это фокусируется на ситуациях, где добавление WLC к сбоям CMX или WLC обнаруживается как недопустимое или неактивное: в основном, когда не подходит NMSP (Протокол сервиса Сетевой мобильности) туннель.

Связь между WLC и CMX происходит с использованием NMSP.

NMSP работает на порте TCP 16113 к WLC и на основе TLS, который требует сертификата (ключевой хэш) обмен между MSE/CMX и контроллером. Туннель TLS/SSL между WLC и CMX инициируется контроллером.

Предварительные условия

Используемые компоненты

CMX 10.2.3-34

WLC 2504 / 8.2.141.0

действительный WLC 8.3.102.0

Установившийся WLC C3650-24TS доступа / 03.06.05E

Требования

Этот документ предполагает, что вы уже знакомы с процессом конфигурирования и руководством по развертыванию. Это фокусируется только на состояниях устранения проблем, где связь NMSP обнаруживается как неактивная

Устранение неисправностей: сценарии возможного сбоя

Первое место для начала является выходными данными следующей команды:

Вход в систему в командной строке CMX и выполненный команда “cmxctl контроллеры config показывает”

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

Кроме того, от выходных данных можно узнать MAC-адрес CMX и ключ Хэша:

Выходные данные, когда будет по крайней мере один неактивный, покажут чек-листа:

1. Достижимость
2. Время
3. Порт SNMP 161
4. Порт NMSP 16113
5. Version
6. Корректный Хэш спешил контроллер

1-Проверяют достижимость

Для проверки достижимости к контроллеру выполняют эхо-запрос от CMX до WLC

2-разовая синхронизация

Оптимальный метод должен указать и CMX и WLC к тому же серверу Протокола NTP.

В Унифицированном WLC (AireOS) это установлено с командой:

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

В установившемся XE IOS доступа:

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

Изменить IP-адрес сервера NTP в CMX:

1. Вход в систему к командной строке как cmxadmin, коммутируйте пользователю маршрута <su root>
2. Остановитесь все сервисы с командой “cmxctl останавливают-a”
3. Однажды весь процесс остановлены, вводят команду “vi/etc/ntp.conf”: нажмите” i”, чтобы переключиться к режиму вставки и изменить IP-адрес, затем нажать “ESC” и тип “: wq” для сохранения конфигурации;
4. Как только параметр изменен, выполните команду “cmxctl перезапуск”, чтобы перезапустить сервисы и переключиться назад cmxadmin пользователю.

Достижимость с 3 SNMP

Чтобы проверить, может ли CMX обратиться к SNMP к WLC, выполните команду в CMX:

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

Вышеупомянутая команда предполагает, что WLC выполняет версию SNMP 2 по умолчанию. В случае, если вы используете версию 3 только, команда была бы похожа:

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

Если SNMP не включен, или название сообщества является неправильным, что будет таймаут. Если успешный, вы будете видеть целое содержание базы данных SNMP WLC.

4-NMSP достижимость

Чтобы проверить, может ли CMX обратиться к NMSP к WLC, выполните команды:

В CMX:

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

В WLC:

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

5 совместимостей версий

Проверьте совместимость версий с последним документом.

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

6-корректный Хэш спешил контроллер

6a), Хэш не представляют на стороне контроллера AireOS

Обычно, wlc добавляют автоматически sha2 и имя пользователя, и ключи могут быть

проверены с командой: 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
```

Если ключ хэша и мак адрес CMX не присутствуют в таблице, то возможно добавить вручную в WLC:

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

6b), Хэш не представляют на стороне контроллера Сходившийся XE IOS доступа

В контроллере NGWC необходимо выполнить команды вручную следующим образом:

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

Примечание: MAC - адрес cmx должен быть добавлен без столбца (:)

Устранять неполадки ключа хэша:

```
 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
```

Проблемы остались?

Если все вышеупомянутое не указывает к проблеме, не стесняйтесь посещать форумы поддержки Cisco для справки (вышеупомянутые выходные данные, и чек-лист определенно поможет сужать вашу проблему на форумах), или откройте запрос Центра технической поддержки!