WLCでのCMX接続のトラブルシューティング

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[考えられる障害シナリオのトラブルシューティング](#)
[到達可能性の確認](#)
[時間同期](#)
[SNMP到達可能性](#)
[NMSP到達可能性](#)
[バージョンの互換性](#)
[コントローラにプッシュされた正しいハッシュ](#)
[コントローラ側AireOSにハッシュが存在しない](#)
[コントローラ側コンバージドアクセスIOS-XEにハッシュが存在しない](#)

概要

このドキュメントでは、UnifiedとConverged with Connected Mobile Experience(CMX)の両方のワイヤレスLANコントローラ(WLC)の接続問題をトラブルシューティングする方法について説明します。

前提条件

要件

設定プロセスと導入ガイドに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CMX 10.2.3-34
- WLC 2504/8.2.141.0
- 仮想WLC 8.3.102.0
- コンバージドアクセスWLC C3650-24TS/03.06.05E

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

注：cmx 10.6を使用している場合は、rootユーザに切り替えるために特別なパッチをインストー

ルする必要があります。Cisco TACに連絡してインストールしてください。

また、ルートパッチを使用する場合でも、完全なパスを使用してコマンドを実行する必要がある場合もあります。「/bin/snmpwalk ...」「snmpwalk」が機能しない場合。

背景説明

この記事では、WLCがCMXに追加されて障害が発生したり、WLCが無効または非アクティブと表示される状況を中心に説明します。基本的に、Network Mobility Service Protocol(NMSP)トンネルが起動しない場合、またはNMSP通信が[Inactive]として表示される場合。

WLCとCMX間の通信は、NMSPを使用して行われます。

NMSPは、WLCに向かうTCPポート16113上で動作し、TLSに基づいて動作します。これには、モビリティサービスエンジン(MSE)/CMXとコントローラ間の証明書（キーハッシュ）交換が必要です。WLCとCMX間のTransport Layer Security/Secure Sockets Layer(TLS/SSL)トンネルは、コントローラによって開始されます。

考えられる障害シナリオのトラブルシューティング

最初に開始する場所は、次のコマンド出力です。

CMXコマンドラインにログインし、コマンド**cmxctl config controllers showを実行します。**

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

また、CMX MACアドレスとハッシュキーは次の出力から見つけることができます。

出力は、少なくとも1つの非アクティブな場合にチェックリストを示します。

1. 到達可能性
2. 時間
3. Simple Network Management Protocol(SNMP)161ポート
4. NMSP 16113ポート
5. バージョン
6. コントローラにプッシュされた正しいハッシュ

到達可能性の確認

コントローラへの到達可能性を確認するには、CMXからWLCにpingを実行します。

時間同期

ベストプラクティスは、CMXとWLCの両方を同じネットワークタイムプロトコル(NTP)サーバにポイントすることです。

Unified WLC(AireOS)では、次のコマンドを使用して設定します。

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

コンバージドアクセスIOS-XEで、次のコマンドを実行します。

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

CMX（CMX 10.6より前）のNTPサーバのIPアドレスを変更するには、次の手順を実行します。

ステップ1：コマンドラインにcmxadminとしてログインし、rootユーザ<su root>に切り替えます。

ステップ2：コマンドcmxctl stop -aを使用してすべてのCMXサービスを停止します。

ステップ3：コマンドservice ntpd stopを使用して、NTPデーモンを停止します。

ステップ4：すべてのプロセスが停止したら、コマンドvi /etc/ntp.confを実行します。iをクリックしてモードを切り替え、IPアドレスを変更し、ESCをクリックし、:wqと入力して設定を保存します。

ステップ5：パラメータを変更したら、コマンドservice ntpd startを実行します。

ステップ6：コマンドntpdate -d <NTP serverのIPアドレス>を使用して、NTPサーバに到達できるかどうかを確認します。

ステップ7:NTPサービスが再起動してntpstatコマンドを使用して確認するまで、少なくとも5分間待ちます。

ステップ8:NTPサーバがCMXと同期したら、コマンドcmxctl restartを実行してCMXサービスを再起動し、cmxadminユーザに切り替える。

CMX 10.6の後は、次のようにCMX NTP設定を確認および変更できます（NTP設定はCMX 10.6以降で有効です）。

ステップ1：コマンドラインにcmxadmin

ステップ2:cmxos health ntpによるNTP同期を確認します。

ステップ 3： NTPサーバを再設定する場合は、cmxos ntp clearを使用し、次にcmxos ntp typeを使用できます。

ステップ4:NTPサーバがCMXと同期したら、コマンドcmxctl restartを実行してCMXサービスを再

起動し、**cmxadminユーザに切り替える。**

SNMP到達可能性

CMXがWLCにSNMPにアクセスできるかどうかを確認するには、CMXで次のコマンドを実行します。

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

このコマンドは、WLCがデフォルトのSNMPバージョン2を実行していることを前提としています。バージョン3では、コマンドは次のようになります。

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

SNMPが有効でない場合、またはコミュニティ名が間違っている場合は、タイムアウトになります。成功すると、WLCのSNMPデータベース全体の内容が表示されます。

> **注：**CMXがWLCサービスポートと同じサブネットにある場合、CMXとWLC間の接続は確立されません。

NMSP到達可能性

CMXがWLCにNMSPにアクセスできるかどうかを確認するには、次のコマンドを実行します。

CMX:

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

WLCで次の操作を行います。

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

バージョンの互換性

最新のドキュメントとのバージョンの互換性を確認します。

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

コントローラにプッシュされた正しいハッシュ

コントローラ側AireOSにハッシュが存在しない

通常、wlcはsha2とユーザ名を自動的に追加します。キーは、**show auth-list**コマンドで確認できます。

```
(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
```

CMXのハッシュキーとMACアドレスがテーブルにない場合、WLCで手動で追加できます。

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

コントローラ側コンバージドアクセスIOS-XEにハッシュが存在しない

NGWCコントローラでは、次のようにコマンドを手動で実行する必要があります。

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

注：cmx mac-addrは、句読点コロン(:)を使用せずに追加する必要があります。

ハッシュキーをトラブルシューティングするには、次の手順を実行します。

```
 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
```

それでも問題が解決しない場合は、シスコのサポートフォーラムを参照してください。この記事に記載されている出力とチェックリストは、フォーラムで問題を絞り込んだり、TACサポートリクエストをオープンしたりするのに役立ちます。