Identificar e Solucionar Problemas de Conectividade CMX com WLC

Contents

Introduction

Este documento descreve os métodos para solucionar problemas de conectividade do Wireless LAN Controller (WLC), tanto Unified quanto Converged with Connected Mobile Experience (CMX).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do processo de configuração e do guia de implantação.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CMX 10.2.3-34
- WLC 2504 / 8.2.141.0
- WLC virtual 8.3.102.0
- Acesso convergido WLC 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Note: se estiver usando o CMX 10.6, será necessário ter um patch especial instalado para poder alternar para o usuário raiz. Entre em contato com o Cisco TAC para instalá-lo.

Além disso, em alguns casos, mesmo com um patch raiz, você precisa executar o comando usando o caminho completo, por exemplo, "/bin/snmpwalk ..." caso "snmpwalk" não funcione.

Informações de Apoio

Este artigo concentra-se em situações em que uma WLC é adicionada ao CMX e falha ou a WLC é exibida como inválida ou inativa. Basicamente, quando o túnel do Network Mobility Service Protocol (NMSP) não é ativado ou as comunicações do NMSP aparecem como Inativas.

A comunicação entre a WLC e o CMX acontece com o uso do NMSP.

O NMSP é executado na porta TCP 16113 em direção à WLC e baseado em TLS, que exige uma troca de certificado (hash chave) entre o Mobility Services Engine (MSE)/CMX e o controlador. O túnel TLS/SSL (Transport Layer Security/Secure Sockets Layer) entre a WLC e o CMX é iniciado pelo controlador.

Solucionar possíveis cenários de falha

O primeiro lugar para iniciar é com esta saída de comando.

Efetue login na linha de comando do CMX e execute o comando **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         |
+------------------+--------------------------------------------------------------------------+
```

Além disso, o endereço MAC do CMX e a chave hash podem ser encontrados na saída:

A saída, quando há pelo menos um inativo, mostra uma lista de verificação:

1. Alcançabilidade
2. Tempo
3. Porta 161 do Simple Network Management Protocol (SNMP)
4. Porta NMSP 16113
5. Versão
6. Hash correto empurrado no controlador

Verificar acessibilidade

Para verificar a acessibilidade ao controlador, execute um ping do CMX para o WLC.

Sincronização de horário

A melhor prática é apontar o CMX e o WLC para o mesmo servidor Network Time Protocol (NTP).

No Unified WLC (AireOS), isso é definido com o comando:

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

No acesso convergido do IOS-XE, execute o comando:

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

Para alterar o endereço IP do servidor NTP no CMX (antes do CMX 10.6):

Etapa 1. Efetue login na linha de comando como **cmxadmin**, mude para o usuário raiz **<su root>**.

Etapa 2. Pare todos os serviços CMX com o comando **cmxctl stop -a**.

Etapa 3. Pare o comando NTP com o comando **service ntpd stop**.

Etapa 4. Quando todo o processo for interrompido, execute o comando **vi /etc/ntp.conf**. Clique em **i** para alternar para o modo de inserção e alterar o endereço IP, depois clique em **ESC** e digite **:wq** para salvar a configuração.

Etapa 5. Depois que o parâmetro for alterado, execute o comando **service ntpd start**.

Etapa 6. Verifique se o servidor NTP está acessível com o comando **ntpdate -d <IP address of NTP server>**.

Passo 7. Aguarde pelo menos cinco minutos para que o serviço NTP reinicie e verifique com o comando **ntpstat**.

Etapa 8. Depois que o servidor NTP for sincronizado com o CMX, execute o comando **cmxctl restart** para reiniciar os serviços do CMX e volte para o usuário **cmxadmin**.

Depois do CMX 10.6, você pode verificar e alterar a configuração do CMX NTP desta maneira :

Etapa 1. Efetue login na linha de comando como **cmxadmin**

Etapa 2. Verifique a sincronização do NTP com o **cmxos health ntp**

Etapa 3. Se quiser reconfigurar o servidor NTP, você pode usar **cmxos ntp clear** e **cmxos ntp type**.

Etapa 4. Depois que o servidor NTP for sincronizado com o CMX, execute o comando **cmxctl restart** para reiniciar os serviços do CMX e volte para o usuário **cmxadmin**.

Alcançabilidade de SNMP

Para verificar se o CMX pode acessar o SNMP para a WLC, execute o comando no CMX:

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

Esse comando pressupõe que a WLC executa a versão 2 do SNMP padrão. Na versão 3, o comando é semelhante a:

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

Se o SNMP não estiver ativado ou o nome da comunidade estiver errado, há um tempo limite. Se for bem-sucedido, você verá todo o conteúdo do banco de dados SNMP da WLC.

> **Note**: A conexão entre CMX e WLC não será estabelecida se o CMX estiver na mesma sub-rede que a porta de serviço do WLC.

Alcançabilidade NMSP

Para verificar se o CMX pode acessar o NMSP para a WLC, execute os comandos:

No CMX:

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

Na WLC:

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

Compatibilidade de versão

Verifique a compatibilidade da versão com o documento mais recente.

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

Hash correto empurrado no controlador

Hash não presente no AireOS do lado do controlador

Geralmente, o wlc adiciona automaticamente o sha2 e o nome de usuário. As chaves podem ser verificadas com o comando **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
```

Se a chave de hash e o endereço MAC do CMX não estiverem presentes na tabela, então é possível adicionar manualmente na WLC:

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

Hash não presente no lado do controlador Acesso convergido IOS-XE

Nos controladores NGWC, você precisa executar os comandos manualmente da seguinte maneira:

```
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 deve ser adicionado sem sinal de pontuação dois-pontos (:)

Para solucionar problemas da chave de hash:

```
 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
```

Se ainda tiver problemas, visite os fóruns de suporte da cisco para obter ajuda. As saídas e a lista de verificação mencionadas neste artigo podem definitivamente ajudá-lo a reduzir seu problema nos fóruns ou você pode abrir uma solicitação de suporte do TAC.