Pesquisando defeitos a Conectividade CMX com WLC

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Pesquisando defeitos encenações da falha possível](#)
[Verifique a alcançabilidade](#)
[Sincronização de tempo](#)
[Alcançabilidade SNMP](#)
[Alcançabilidade NMSP](#)
[Compatibilidade de versão](#)
[Mistura correta empurrada no controlador](#)
[Mistura não atual no lado AireOS do controlador](#)
[A mistura não atual no lado do controlador convirgiu o acesso IOS-XE](#)

Introdução

Este documento descreve os métodos para pesquisar defeitos os problemas de conectividade do controlador do Wireless LAN (WLC), unificado e convirgido com experiência móvel conectada (CMX).

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do processo de configuração e do guia de distribuição.

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 convirgido WLC C3650-24TS/03.06.05E

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o

impacto potencial do comando any.

Informações de Apoio

Este artigo centra-se sobre as situações onde um WLC é adicionado ao CMX e falha, ou o WLC aparece como inválido ou inativo. Basicamente quando o túnel do protocolo de serviço da mobilidade da rede (NMSP) não vem acima ou as comunicações NMSP aparece como inativo.

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

NMSP é executado na porta TCP 16113 para o WLC e baseados no TLS, que exige uma troca do certificado (mistura chave) entre o motor dos Serviços de mobilidade (MSE) /CMX e o controlador. O túnel do Transport Layer Security/secure sockets layer (TLS/SSL) entre o WLC e CMX é iniciado pelo controlador.

Pesquisando defeitos encenações da falha possível

O primeiro lugar a começar é com esta saída do comando.

O log na linha de comando CMX e executado os **controladores da configuração do cmxctl do** comando **mostra**.

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

Também, o MAC address CMX e a Mistura-chave podem ser encontrados da saída:

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

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

Verifique a alcançabilidade

A fim verificar a alcançabilidade ao controlador, execute um sibilo de CMX ao WLC.

Sincronização de tempo

O melhor prática é apontar ambo o CMX e o WLC ao mesmo server do Network Time Protocol (NTP).

Em WLC unificado (AireOS), isto é ajustado com o comando:

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

No acesso convirgido IOS-XE, execute o comando:

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

A fim mudar o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de NTP em CMX:

Etapa 1. Log na linha de comando como o **cmxadmin**, interruptor ao **root> do <**su do usuário de raiz.

Etapa 2. Pare todos os serviços CMX com a **parada do cmxctl do** comando **- a**.

Etapa 3. Pare o deamon NTP com a **parada do ntpd do** comando service.

Etapa 4. Uma vez que todo o processo é parado, execute o comando vi **/etc/ntp.conf**. Clique **i** para comutar ao modo inserido e para mudar o endereço IP de Um ou Mais Servidores Cisco ICM NT, a seguir para clicar o **ESC** e datilografá-lo**: wq** para salvar a configuração.

Etapa 5. Uma vez que o parâmetro é mudado execute o **começo do ntpd do** comando service.

Etapa 6. Verifique se o servidor de NTP é alcançável com o **ntpdate do** comando **- d < endereço IP de Um ou Mais Servidores Cisco ICM NT do server> NTP**.

Etapa 7. Permita que cinco minutos pelo menos, porque o serviço NTP reiniciem e verifiquem com o **ntpstat do** comando.

Etapa 8. Uma vez que o servidor de NTP é sincronizado com o CMX, execute o **reinício do cmxctl do** comando para reiniciar os serviços CMX e o interruptor de volta ao usuário do **cmxadmin**.

Alcançabilidade SNMP

A fim verificar se CMX podem alcançar o SNMP ao WLC, execute o comando em CMX:

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

Este comando supõe que o WLC executa a versão de SNMP 2. do padrão. Na versão 3, o comando olha como:

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

```
127.0.0.1:161 system
```

Se o SNMP não é permitido, ou o nome da comunidade é erro lá é um intervalo. Se é bem sucedido, você vê o índice inteiro do base de dados SNMP do WLC.

Alcançabilidade NMSP

A fim verificar se CMX podem alcançar NMSP ao WLC, execute os comandos:

Em CMX:

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

No WLC:

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

Compatibilidade de versão

Verifique a compatibilidade de versão com o documento o mais atrasado.

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

Mistura correta empurrada no controlador

Mistura não atual no lado AireOS do controlador

Geralmente, o wlc adiciona automaticamente o sha2 e o username. As chaves podem ser verificadas com a autêntico-**lista do** comando show.

```
(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 da mistura e o MAC address de CMX não estão atuais na tabela, a seguir é possível adicionar manualmente no WLC:

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

A mistura não atual no lado do controlador convirgiu o acesso IOS-XE

Em controladores NGWC, você precisa de executar manualmente os comandos como segue:

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

Note: o MAC-ADDR cmx deve ser adicionado sem dois pontos da marca de pontuação (:)

A fim pesquisar defeitos a chave da mistura:

```
 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 você ainda enfrenta quaisquer edições, visite fóruns do apoio de Cisco para a ajuda. As saídas e a lista de verificação mencionadas neste artigo podem definidamente ajudá-lo a reduzir para baixo seu problema nos fóruns ou você pode abrir um pedido do suporte de TAC.