Pesquisando defeitos a Conectividade CMX com WLC

Índice

Introdução

Este documento analisa os métodos para pesquisar defeitos os problemas de conectividade do controlador do Wireless LAN (WLC): unificado e convirgido com experiência móvel conectada (CMX). Centra-se sobre as situações onde adicionar um WLC ao CMX falha ou o WLC aparece como inválido ou inativo: basicamente quando o túnel NMSP (protocolo de serviço da mobilidade da rede) não vier acima.

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 MSE/CMX e o controlador. O túnel TLS/SSL entre o WLC e CMX é iniciado pelo controlador.

Pré-requisitos

Componentes usados

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

Requisitos

Este documento supõe que você é já familiar com o processo de configuração e o guia de distribuição. Centra-se somente sobre as situações de Troubleshooting onde as comunicações NMSP aparecem como inativo

Troubleshooting: encenações da falha possível

O primeiro lugar a começar é o comando seguinte output:

Entre na linha de comando CMX e execute o comando do “mostra dos controladores da configuração cmxctl”

```
** 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, da saída você pode encontrar o MAC address CMX e a Mistura-chave:

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

1. Alcançabilidade
2. Tempo
3. Porta SNMP 161
4. Porta NMSP 16113
5. Versão
6. Mistura correta empurrada no controlador

1- Verifique a alcançabilidade

Para verificar a alcançabilidade ao controlador emita um sibilo de CMX ao WLC

sincronização 2-Time

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:

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

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

1. Início de uma sessão à linha de comando como o cmxadmin, interruptor ao root> do <su do usuário de raiz
2. Pare todos os serviços com o comando do “parada cmxctl -”
3. Uma vez que todo o processo é parado, incorpore o comando “vi /etc/ntp.conf”: pressione-me “” comutar ao modo inserido e mudar o endereço IP de Um ou Mais Servidores Cisco ICM NT, a seguir para pressionar o “ESC” e para datilografá-lo “: wq” para salvar a configuração;
4. Uma vez que o parâmetro é mudado, emita o comando do “reinício cmxctl” reiniciar os serviços e o interruptor de volta ao usuário do cmxadmin.

Alcançabilidade 3-SNMP

Para verificar se CMX podem alcançar o SNMP ao WLC, emita o comando em CMX:

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

O comando acima supõe que o WLC executa a versão de SNMP 2. do padrão caso que você usa a versão 3 somente, o comando olharia 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 errado lá será um intervalo. Se bem sucedido, você verá o índice inteiro do base de dados SNMP do WLC.

Alcançabilidade 4-NMSP

Para verificar se CMX podem alcançar NMSP ao WLC, emita os comandos:

Em CMX:

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

No WLC:

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

compatibilidade 5-Version

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 6-Correct empurrada no controlador

6a) **Pique não atual no lado AireOS do controlador**

Geralmente, o wlc adiciona automaticamente o sha2 e o username e as chaves podem ser verificadas com o comando: mostre a autêntico-lista

```
(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>
```

6b) **Pique não atual no controlador que o lado convirgiu o acesso IOS-XE**

No controlador 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 >
```

Nota: o MAC-ADDR cmx deve ser adicionado sem coluna (:)

Para 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
```

Ainda tendo problemas?

Se todos os acima não apontam ao problema, para sentir livres visitar fóruns do apoio de Cisco para a ajuda (as saídas e a lista de verificação acima ajudarão definidamente a reduzir para baixo seu problema nos fóruns) ou a abrir um pedido do suporte de TAC!