Compreenda e pesquise defeitos a autenticação da Web central (CWA) na instalação da âncora do convidado

Índice

Introdução

Este documento descreve como o webauth central trabalha em uma âncora do convidado setup e alguns dos problemas comuns considerados em uma rede de produção e como podem ser fixos.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento em como configurar o webauth central no controlador do Wireless LAN (WLC).

Este documento fornece etapas a propósito da configuração do webauth central: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

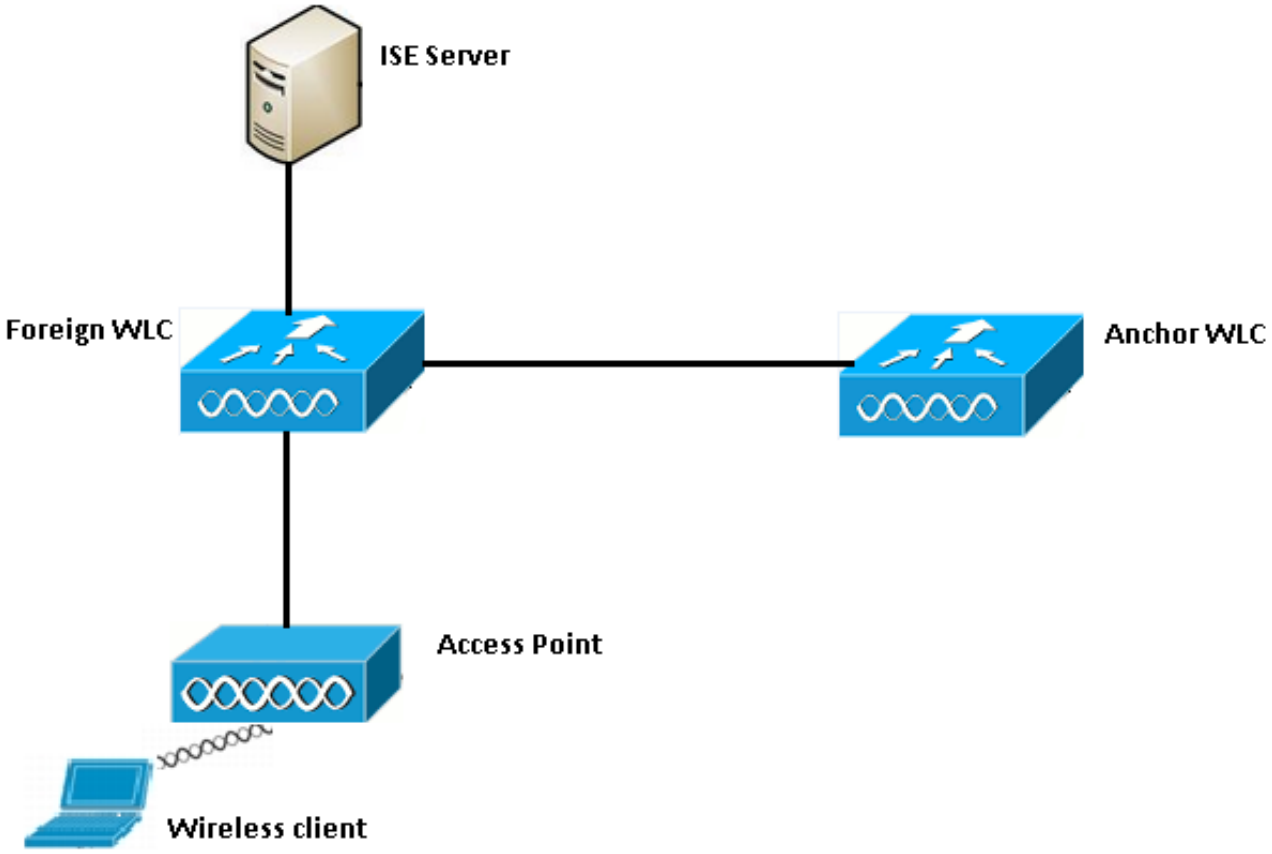
Componentes Utilizados

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

- Versão 7.6 running WLC 5508
- Versão 1.4 running do Identity Services Engine (ISE)

Fluxo básico

Esta seção mostra os trabalhos básicos do webauth central em uma âncora do convidado setup segundo as indicações da imagem:



Etapa 1. O cliente começa a conexão quando envia um pedido da associação.

Etapa 2. O WLC começa o processo de autenticação de MAC quando envia um pedido de autenticação ao server ISE configurado.

Etapa 3. Baseado na política da autorização configurada no ISE, a mensagem da aceitação de acesso é enviada para trás ao WLC com a reorientação URL e reorienta entradas do Access Control List (ACL).

Etapa 4. O WLC estrangeiro envia então uma resposta da associação ao cliente.

Etapa 5. Esta informação é passada sobre pelo WLC estrangeiro à âncora WLC em mensagens da entrega da mobilidade. Você precisa de assegurar-se de que a reorientação ACL esteja configurada na âncora e em WLC estrangeiros.

Etapa 6. Nesta fase, o cliente move-se no estado de corrida no WLC estrangeiro.

Etapa 7. Uma vez que o cliente inicia o Web-AUTH com uma URL no navegador, a âncora começa o processo de redirecionamento.

Etapa 8. Uma vez que o cliente é autenticado com sucesso, o cliente move-se no estado de **CORRIDA na** âncora WLC.

Fluxo central de Webauth para a tentativa bem sucedida da conexão de cliente

Você pode agora analisar o fluxo básico descrito acima em detalhe quando você atravessa debuga. Estes debugam foram recolhidos na âncora e no WLC estrangeiro para ajudar com sua análise:

```
debug client 00:17:7c:2f:b8:6e
debug aaa detail enable
debug mobility handoff enable
debug web-auth redirect enable mac 00:17:7c:2f:b8:6e
```

Estes detalhes são usados aqui:

```
WLAN name: CWA
WLAN ID: 5
IP address of anchor WLC: 10.105.132.141
IP address of foreign WLC: 10.105.132.160
Redirect ACL used: REDIRECT
Client MAC address: 00:17:7c:2f:b8:6e
New mobility architecture disabled
```

Etapa 1. O cliente começa o processo da conexão quando envia um pedido da associação. Isto é visto no controlador estrangeiro:

```
*apfMsConnTask_6: May 08 12:10:35.897: 00:17:7c:2f:b8:6e Association received from mobile on
BSSID dc:a5:f4:ec:df:34
```

Etapa 2. O WLC vê que o Wireless LAN (WLAN) está traçado para a autenticação de MAC e move o cliente para o **status pendente AAA**. Igualmente começa o processo de autenticação quando envia um pedido de autenticação ao ISE:

```
*apfMsConnTask_6: May 08 12:10:35.898: 00:17:7c:2f:b8:6e apfProcessAssocReq (apf_80211.c:8221)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Idle to AAA Pending
*aaaQueueReader: May 08 12:10:35.898: AuthenticationRequest: 0x2b6bf574

*aaaQueueReader: May 08 12:10:35.898: Callback.....................................0x10166e78
*aaaQueueReader: May 08 12:10:35.898: protocolType.................................0x40000001
*aaaQueueReader: May 08 12:10:35.898:
proxyState.....................................00:17:7C:2F:B8:6E-00:00
```

Etapa 3. No ISE, o desvio da autenticação de MAC é configurado e retorna a reorientação URL e ACL após a autenticação de MAC. Você pode ver estes parâmetros enviados na resposta de autorização:

```
*radiusTransportThread: May 08 12:10:35.920: AuthorizationResponse: 0x14c47c58
*radiusTransportThread: May 08 12:10:35.920: structureSize...............................320
*radiusTransportThread: May 08 12:10:35.920: resultCode...................................0
*radiusTransportThread: May 08 12:10:35.920:
protocolUsed.................................0x00000001
*radiusTransportThread: May 08 12:10:35.920:
proxyState.....................................00:17:7C:2F:B8:6E-00:00
*radiusTransportThread: May 08 12:10:35.920: Packet contains 5 AVPs:
*radiusTransportThread: May 08 12:10:35.920: AVP[01] User-
```

```
Name.............................00-17-7C-2F-B8-6E (17 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[02]
State.................................ReauthSession:0a6984a00000004c536bac7b (38 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[03]
Class.................................CACS:0a6984a00000004c536bac7b:sid-ise-1-2/188796966/38
(54 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[04] Cisco / Url-Redirect-
Acl..............REDIRECT (8 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[05] Cisco / Url-
Redirect...................DATA (91 bytes)
```

Você pode ver a mesma informação sob os logs ISE. Navegue aos **>Authentications das operações** e clique **detalhes da sessão cliente** segundo as indicações da imagem:

Result

User-Name	00-17-7C-2F-B8-6E
State	ReauthSession:0a6984a0000000045371b7c4
Class	CACS:0a6984a0000000045371b7c4:sid-ise-1-2/188796966/714
cisco-av-pair	url-redirect-acl=REDIRECT
cisco-av-pair	url-redirect=https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a0000000045371b7c4&action=cwa

Etapa 4. O WLC estrangeiro então muda o estado ao AUTH L2 completo e envia a resposta da associação ao cliente.

> **Note**: Com a autenticação de MAC permitida, a resposta da associação não é enviada até que esta esteja terminada.

```
*apfReceiveTask: May 08 12:10:35.921: 00:17:7c:2f:b8:6e 0.0.0.0 AUTHCHECK (2) Change state to
L2AUTHCOMPLETE (4)
*apfReceiveTask: May 08 12:10:35.922: 00:17:7c:2f:b8:6e Sending Assoc Response to station on
BSSID dc:a5:f4:ec:df:34 (status 0) ApVapId 5 Slot 0
```

Passo 5: O estrangeiro inicia então o processo da entrega à âncora. Isto é visto a entrega da mobilidade debugar output:

```
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e Attempting anchor export for mobile
00:17:7c:2f:b8:6e
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e Anchor Export:
Client IP: 0.0.0.0, Anchor IP: 10.105.132.141
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e mmAnchorExportSend: Building
UrlRedirectPayload
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e Anchor Export: Sending url redirect acl
REDIRECT
```

Etapa 6. Você pode ver que o cliente se move no estado de CORRIDA no WLC estrangeiro. O status correto do cliente pode agora ser considerado somente na âncora. Está aqui um snippet da saída do detalhe do cliente da mostra recolhida do estrangeiro (somente a informação relevante é mostrada):

```
Client MAC Address.............................. 00:17:7c:2f:b8:6e
Client Username ................................ 00-17-7C-2F-B8-6E
AP MAC Address.................................. dc:a5:f4:ec:df:30
BSSID........................................... dc:a5:f4:ec:df:34
IP Address...................................... Unknown
Gateway Address................................. Unknown
Netmask......................................... Unknown
Mobility State.................................. Export Foreign
Mobility Anchor IP Address...................... 10.105.132.141
Policy Manager State............................ RUN
Policy Manager Rule Created..................... Yes
AAA Override ACL Name........................... REDIRECT
AAA URL
redirect.............................https://10.106.73.98:8443/guestportal/gatewaysessionId=
0a6984a00000004c536bac7b&action=cwa
```

Etapa 7. O controlador estrangeiro inicia um pedido da entrega com a âncora. Você pode agora ver as mensagens da entrega abaixo:

```
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e Received Anchor Export request: from Switch
IP: 10.105.132.160
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e Adding mobile on Remote AP
00:00:00:00:00:00(0)
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv:, Mobility role is Unassoc
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv Ssid=cwa Security
Policy=0x42000
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv vapId= 5, Ssid=cwa
AnchorLocal=0x0
*mmListen: May 08 05:52:50.588: 00:17:7c:2f:b8:6e mmAnchorExportRcv:Url redirect
https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a00000004c536bac7b&action=cwa
*mmListen: May 08 05:52:50.588: 00:17:7c:2f:b8:6e Url redirect ACL REDIRECT

A handoff acknowledgement message is also sent to the foreign and can be seen in the debugs on
foreign:
*mmListen: May 08 12:10:38.802: 00:17:7c:2f:b8:6e Received Anchor Export Ack for client from
Switch IP: 10.105.132.141
*mmListen: May 08 12:10:38.802: 00:17:7c:2f:b8:6e Anchor Mac: d0:c2:82:e2:91:60, Old Foreign
Mac: 30:e4:db:1b:e0:a0 New Foreign Mac: 30:e4:db:1b:e0:a0
```

Etapa 8. O controlador da âncora move então o cliente para o estado exigido DHCP. Uma vez que o cliente obtém um endereço IP de Um ou Mais Servidores Cisco ICM NT, o controlador continua a processar e mover o cliente webauth central no estado exigido. Você pode ver o mesmos na saída do detalhe do cliente da mostra recolhida na âncora:

```
Client MAC Address.............................. 00:17:7c:2f:b8:6e
AP MAC Address.................................. 00:00:00:00:00:00
Client State.................................... Associated
Wireless LAN Id................................. 5
IP Address...................................... 10.105.132.254
Mobility State.................................. Export Anchor
Mobility Foreign IP Address..................... 10.105.132.160
Policy Manager State............................ CENTRAL_WEB_AUTH
AAA Override ACL Name........................... REDIRECT
AAA URL redirect.............................
https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a00000004c536bac7b&action=cwa
```

Etapa 9. O WLC estrangeiro começa simultaneamente o processo da contabilidade uma vez que move o cliente no estado de corrida. Envia a mensagem do começo da contabilidade ao ISE:

```
*aaaQueueReader: May 08 12:10:38.803: AccountingMessage Accounting Start: 0x2b6c0a78
*aaaQueueReader: May 08 12:10:38.803: Packet contains 16 AVPs:
*aaaQueueReader: May 08 12:10:38.803: AVP[01] User-Name.............................00-17-7C-
2F-B8-6E (17 bytes)
```

Note: Explicar precisa somente de ser configurado no WLC estrangeiro.

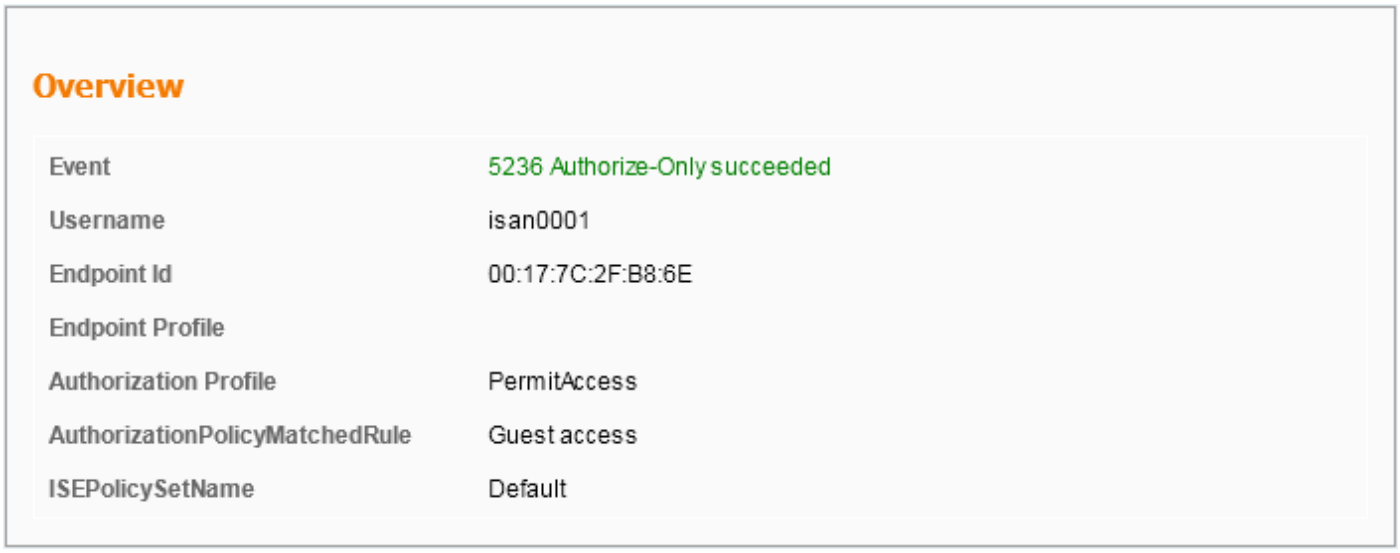
Etapa 10. O usuário inicia então o Web-AUTH reorienta o processo incorporando uma URL ao navegador. Você pode ver que o relevante debuga no controlador da âncora:

```
*webauthRedirect: May 08 05:53:05.927: 0:17:7c:2f:b8:6e- received connection
*webauthRedirect: May 08 05:53:05.928: captive-bypass detection disabled, Not checking for wispr
in HTTP GET, client mac=0:17:7c:2f:b8:6e
*webauthRedirect: May 08 05:53:05.928: 0:17:7c:2f:b8:6e- Preparing redirect URL according to
configured Web-Auth type
*webauthRedirect: May 08 05:53:05.928: 0:17:7c:2f:b8:6e: Client configured with AAA overridden
redirect URL
https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a00000004c536bac7b&action=cwa
```

Etapa 11. Nós podemos igualmente ver que a peça da autenticação no processo do webauth está segurada no WLC estrangeiro e não na âncora. Você pode ver o mesmos nas saídas debugar AAA no estrangeiro:

```
*aaaQueueReader: May 08 12:11:11.537: AuthenticationRequest: 0x2b6c0a78
*aaaQueueReader: May 08 12:11:11.537: Callback.....................................0x10166e78
*aaaQueueReader: May 08 12:11:11.537: protocolType.................................0x40000001
*aaaQueueReader: May 08 12:11:11.537:
proxyState.....................................00:17:7C:2F:B8:6E-00:00
*aaaQueueReader: May 08 12:11:11.537: Packet contains 12 AVPs (not shown)
Authorization response from ISE:
*radiusTransportThread: May 08 12:11:11.552: AuthorizationResponse: 0x14c47c58
*radiusTransportThread: May 08 12:11:11.552: structureSize.............................252
*radiusTransportThread: May 08 12:11:11.552: resultCode.................................0
*radiusTransportThread: May 08 12:11:11.552:
protocolUsed.................................0x00000001
*radiusTransportThread: May 08 12:11:11.552:
proxyState.....................................00:17:7C:2F:B8:6E-00:00
*radiusTransportThread: May 08 12:11:11.552: Packet contains 6 AVPs:
*radiusTransportThread: May 08 12:11:11.552: AVP[01] User-
Name.............................isan0001 (8 bytes) -----> (Username used for web
authentication)
*radiusTransportThread: May 08 12:11:11.552: AVP[02]
State.....................................ReauthSession:0a6984a00000004c536bac7b (38 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[03]
Class.....................................CACS:0a6984a00000004c536bac7b:sid-ise-1-2/188796966/40
(54 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[04] Session-
Timeout.........................0x00006e28 (28200) (4 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[05] Termination-
Action.....................0x00000000 (0) (4 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[06] Message-
Authenticator...................DATA (16 bytes)
```

O mesmos podem ser verificados no ISE segundo as indicações da imagem:



Etapa 12. Esta informação é passada na âncora WLC. Este aperto de mão não é claramente visível no debuga e você pode fazer este para fora pela âncora que aplica uma política da entrega do cargo como mostrado aqui:

```
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e Received Anchor Export policy update, valid
mask 0x900:
Qos Level: 0, DSCP: 0, dot1p: 0 Interface Name: , IPv4 ACL Name:
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e Applying post-handoff policy for station
00:17:7c:2f:b8:6e - valid mask 0x900
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e QOS Level: -1, DSCP: -1, dot1p: -1,
Data Avg: -1, realtime Avg: -1, Data Burst -1, Realtime Burst -1
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e Session: 0, User session: 28200, User elapsed
1
Interface: N/A, IPv4 ACL: N/A, IPv6 ACL: N/A.
```

A melhor maneira de verificar que a autenticação está completa é verificar que passado entra o ISE e recolhe a saída do detalhe do cliente da mostra no controlador que deve mostrar o cliente no estado de **CORRIDA** como mostrado aqui:

```
Client MAC Address.............................. 00:17:7c:2f:b8:6e
Client State.................................... Associated
Client NAC OOB State............................ Access
Wireless LAN Id................................. 5
IP Address...................................... 10.105.132.254
Mobility State.................................. Export Anchor
Mobility Foreign IP Address..................... 10.105.132.160
Policy Manager State............................ RUN
```

Uma outra verificação importante é o fato de que a âncora envia um protocolo gratuito de resolução de endereço (ARP) após a autenticação bem sucedida:

```
*pemReceiveTask: May 08 05:53:23.343: 00:17:7c:2f:b8:6e Sending a gratuitous ARP for
10.105.132.254, VLAN Id 20480
```

Aqui do cliente está livre enviar todos os tipos de tráfego que é enviado para fora pelo controlador da âncora.

Fluxo central de Webauth quando o cliente obtiver desligado

Quando uma entrada de cliente precisa de ser removida do WLC ou devido a uma sessão/idle timeout ou quando nós removemos manualmente o cliente do WLC, estas etapas ocorrem:

O WLC estrangeiro envia uma mensagem da de-autenticação ao cliente e programa-a para o supressão:

```
*apfReceiveTask: May 08 12:19:21.199: 00:17:7c:2f:b8:6e apfMsExpireMobileStation (apf_ms.c:6634)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Associated to
Disassociated
*apfReceiveTask: May 08 12:19:21.199: 00:17:7c:2f:b8:6e Sent Deauthenticate to mobile on BSSID
dc:a5:f4:ec:df:30 slot 0(caller apf_ms.c:6728
```

Envia então uma mensagem da contabilidade da parada do raio para informar o server ISE que a sessão da authenticação do cliente terminou:

```
*aaaQueueReader: May 08 12:19:21.199: AccountingMessage Accounting Stop: 0x2b6d5684
*aaaQueueReader: May 08 12:19:21.199: Packet contains 24 AVPs:
*aaaQueueReader: May 08 12:19:21.199: AVP[01] User-Name.............................00-17-7C-
2F-B8-6E (17 bytes)
```

Igualmente envia uma mensagem da entrega da mobilidade à âncora WLC para informá-la para terminar a sessão cliente. Isto pode ser visto na mobilidade debuga na âncora WLC:

```
*mmListen: May 08 06:01:32.907: 00:17:7c:2f:b8:6e Received Handoff End request for client from
Switch IP: 10.105.132.160
*apfReceiveTask: May 08 06:01:32.907: 00:17:7c:2f:b8:6e apfMmProcessResponse: Handoff end rcvd
for mobile 00:17:7c:2f:b8:6e, delete mobile. reason code = 0
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e 10.105.132.254 RUN (20) mobility role
update request from Export Anchor to Handoff
Peer = 10.105.132.160, Old Anchor = 10.105.132.141, New Anchor = 0.0.0.0
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e apfMmProcessCloseResponse (apf_mm.c:647)
Expiring Mobile!
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e Mobility Response: IP 0.0.0.0 code
Anchor Close (5), reason Normal disconnect (0), PEM State DHCP_REQD, Role Handoff(6)
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e Deleting mobile on AP
00:00:00:00:00:00(0)
```

Conta do cliente suspendida no ISE

O ISE tem a capacidade para suspender uma conta de usuário convidado que sinalize o WLC para terminar a sessão cliente. Isto é útil para os administradores que não precisam de verificar que WLC o cliente é conectado e de terminar simplesmente a sessão. Você pode agora ver o que acontece quando a conta de usuário convidado é suspendida/expirada no ISE:

O server ISE envia uma mudança da mensagem da autorização ao controlador estrangeiro que indica que a conexão de cliente precisa de ser removida. Isto pode ser visto nos resultados do debug:

```
*radiusCoASupportTransportThread: May 13 02:01:53.446: 00:17:7c:2f:b8 :6e apfMsDeleteByMscb
Scheduling mobile for deletion with deleteReason 6, reason Code 252
*radiusCoASupportTransportThread: May 13 02:01:53.446: 00:17:7c:2f:b8:6e Schedul ing deletion of
Mobile Station: (callerId: 30) in 1 seconds
```

O WLC estrangeiro envia então uma mensagem da de-autenticação ao cliente:

```
*apfReceiveTask: May 13 02:01:54.303: 00:17:7c:2f:b8:6e Sent Deauthenticate to mobile on BSSID
dc:a5:f4:ec:df:30 slot 0(caller apf_ms.c:5921)
```

Igualmente envia uma mensagem da parada da contabilidade ao servidor de contabilidade para terminar a sessão da authenticação do cliente em seu lado:

```
*aaaQueueReader: May 13 02:01:54.303: AccountingMessage Accounting Stop: 0x2b6d2 c7c
*aaaQueueReader: May 13 02:01:54.303: Packet contains 23 AVPs:
*aaaQueueReader: May 13 02:01:54.303: AVP[01] User-Name.....................
.............00177c2fb86e (12 bytes)
```

Uma mensagem da entrega é enviada igualmente à âncora WLC para terminar a sessão cliente. Você pode ver este na âncora WLC:

```
*mmListen: May 12 19:42:52.871: 00:17:7c:2f:b8:6e Received Handoff End request for client from
Switch IP: 10.105.132.160
*apfReceiveTask: May 12 19:42:52.872: 00:17:7c:2f:b8:6e apfMmProcessResponse: Handoff end rcvd
for mobile 00:17:7c:2f:b8:6e, delete mobile. reason code = 0
```

Pesquise defeitos Webauth central na instalação da âncora do convidado

Deixe-nos agora ter um olhar em alguns dos problemas comuns vistos quando você usa CWA e o que pode ser feito para o fixar.

O cliente da encenação 1. colado no estado do COMEÇO e não obtém o endereço IP de Um ou Mais Servidores Cisco ICM NT

Em uma encenação central do webauth desde que a autenticação de MAC é permitida, as respostas da associação são enviadas depois que uma autenticação de MAC é terminada. Neste caso, se há uma falha de comunicação entre o WLC e o servidor Radius ou há um misconfig no servidor Radius que faz com que envie rejeições de acesso, você pode ver o cliente colado em uma associação para dar laços em onde obtém repetidamente uma rejeição da associação. Há igualmente uma possibilidade que o cliente obtenha excluído também se a exclusão do cliente é permitida.

A alcançabilidade do servidor Radius pode ser verificada com o comando dos **radius AAA do teste** que está disponível no código 8.2 e acima.

O link de referência abaixo mostra como usar isto:
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212473-verify-radius-server-connectivity-with-t.html

O cliente da encenação 2. é incapaz de obter o endereço IP de Um ou Mais Servidores Cisco ICM NT

Há algumas razões pelas quais um cliente pode não obtém um endereço IP de Um ou Mais Servidores Cisco ICM NT em uma instalação da âncora do convidado CWA.

- **A configuração SSID na âncora e estrangeiro não combinam**

Éideal ter a configuração SSID mesmos entre a âncora e os WLC estrangeiros. Alguns dos

aspectos para que uma verificação estrita é feita são configuração da Segurança L2/L3, configuração DHCP e de ultrapassagem AAA parâmetros. Caso que este não é o mesmo, uma entrega à âncora falha e você pode ver que estas mensagens na âncora debugam:

```
DHCP dropping packet due to ongoing mobility handshake exchange, (siaddr 0.0.0.0, mobility state
= 'apfMsMmAnchorExportRequested'
```

A fim abrandar isto, você precisa de assegurar-se de que a configuração SSID seja a mesma âncora e estrangeira.

- **O túnel da mobilidade entre a âncora e WLC estrangeiros é abaixo de/flapping**

Todo o tráfego do cliente é enviado no túnel dos dados da mobilidade que usa o protocolo IP 97. Se o túnel da mobilidade não é acima de então você pode ver que a entrega não termina e o cliente não se move no estado de CORRIDA no estrangeiro. O status de túnel da mobilidade precisa de mostrar como **ACIMA** e pode ser considerado sob **grupos do >Mobility do Gerenciamento do >Mobility do controlador** segundo as indicações da imagem.

Se há somente um controlador traçado como um membro (estrangeiro ou âncora), a seguir você pode igualmente verificar as estatísticas globais da mobilidade sob **estatísticas do >Statistics > da mobilidade do monitor.**

- **Reoriente o ACL não configurado na âncora ou em controladores estrangeiros:**

Quando o nome da reorientação ACL enviada pelo servidor Radius não combina o que está configurado no WLC estrangeiro, a seguir mesmo que a autenticação de MAC seja terminada, o cliente é rejeitado e não continua fazer o DHCP. Não é imperativo configurar as regras ACL individuais porque o tráfego do cliente é terminado na âncora. Enquanto há um ACL criado com o mesmo nome que a reorientação ACL, o cliente está entregado fora à âncora. A âncora precisa de ter o nome e as regras ACL configurados corretamente para que o cliente mova-se para o estado exigido webauth.

O cliente da encenação 3. não obtém reorientado ao página da web

Há outra vez algumas razões diferentes pelas quais uma página do webauth pode não obtém indicada. Algumas das edições laterais comuns WLC são cobertas aqui:

- **Edições do servidor DNS**

As edições da alcançabilidade/misconfig do servidor DNS são um da maioria de motivos comuns pelas quais os clientes não obtêm reorientados. Isto pode igualmente ser duro de travar porque não aparece em nenhuns logs WLC nem debuga. O usuário precisa de verificar se a configuração do servidor DNS empurrada do servidor DHCP está correta e se é alcançável do cliente Wireless. Uma pesquisa de DNS simples do cliente detrabalho é a maneira a mais fácil de verificar isto.

- **Gateway padrão un-alcançável quando você usar o servidor DHCP interno na âncora:**

Quando você usa servidores DHCP internos, é importante assegurar-se de que a configuração do gateway padrão esteja correta e o VLAN esteja permitido no switchport que conecta à âncora WLC. Se não, o cliente obtém um endereço IP de Um ou Mais Servidores Cisco ICM NT, mas não poderá alcançar qualquer coisa. Você pode verificar a tabela ARP no cliente para ver se há o MAC address do gateway. É uma maneira rápida verificar que a Conectividade L2 ao gateway e àquele ele é alcançável.