Comprenez et dépannez l'authentification Web centrale (CWA) dans l'installation d'ancre d'invité

Contenu

Introduction

Ce document décrit comment les travaux centraux de webauth dans un invité ancrent l'installation et certains des problèmes courants vus dans un réseau de production et comment ils peuvent être réparés.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance sur la façon dont configurer le webauth central sur le contrôleur LAN Sans fil (WLC).

Ce document fournit des étapes quant à la configuration du webauth central : https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

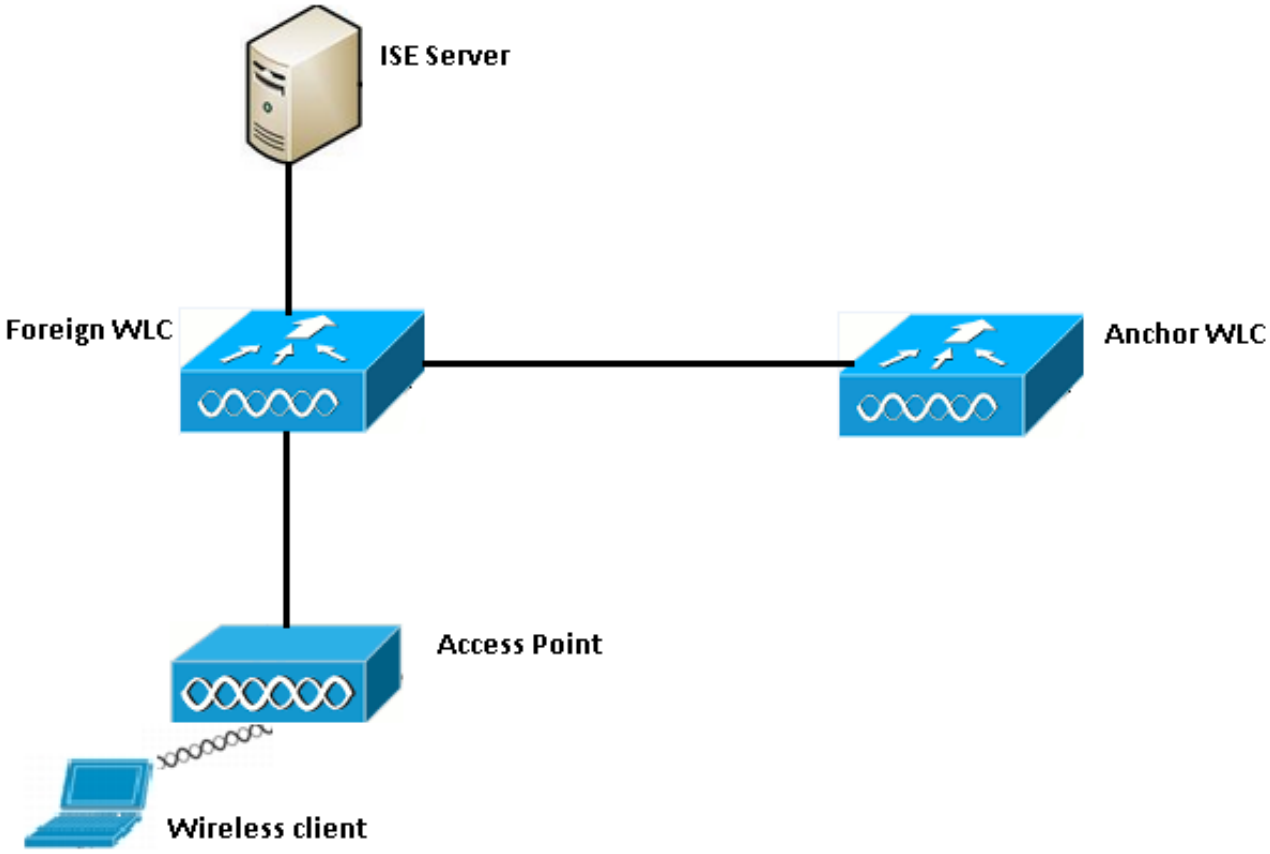
Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 7.6 courante WLC 5508
- Version 1.4 courante du Cisco Identity Services Engine (ISE)

Écoulement de base

Cette section affiche le processus de base du webauth central dans une ancre d'invité installée suivant les indications de l'image :



Étape 1. Le client commence la connexion quand il envoie une demande d'association.

Étape 2. WLC commence le procédé d'authentification MAC quand il envoie une demande d'authentification au serveur ISE configuré.

Étape 3. Basé sur la stratégie configurée d'autorisation sur ISE, le message d'Access-recevoir est renvoyé au WLC avec l'URL de réorientation et réoriente des entrées de liste de contrôle d'accès (ACL).

Étape 4. Le WLC étranger envoie alors une réponse d'association au client.

Étape 5. Ces informations sont transmises par le WLC étranger à l'ancre WLC dans des messages de transfert de mobilité. Vous devez s'assurer que la réorientation ACL sont configurées sur l'ancre et WLC étrangers.

Étape 6. À ce stade, le client entre dans l'état de passage sur le WLC étranger.

Étape 7. Une fois que le client initie le Web-auth avec un URL dans le navigateur, l'ancre commence le procédé de redirection.

Étape 8. Une fois que le client est avec succès authentifié, le client entre dans l'état de **PASSAGE** sur l'ancre WLC.

Écoulement central de Webauth pour la tentative réussie de

connexion client

Vous pouvez maintenant analyser l'écoulement de base décrit ci-dessus en détail quand vous passez par met au point. Ceux-ci met au point ont été collectés sur l'ancre et WLC étranger pour aider avec votre analyse :

```
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
```

Ces détails sont utilisés ici :

```
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
```

Étape 1. Le client commence la procédure de connexion quand il envoie une demande d'association. Ceci est vu sur le contrôleur étranger :

```
*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
```

Étape 2. Le WLC voit que le RÉSEAU LOCAL Sans fil (WLAN) est tracé pour l'authentification MAC et déplace le client à l'état **en attendant d'AAA**. Il commence également la procédure d'authentification quand il envoie une demande d'authentification à 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
```

Étape 3. Sur l'ISE, le contournement d'authentification MAC est configuré et il renvoie l'URL de réorientation et l'ACL après authentification MAC. Vous pouvez voir ces paramètres introduits la réponse d'autorisation :

```
*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)
```

Vous pouvez voir les mêmes informations sous les logs ISE. Naviguez vers des **>Authentications d'exécutions** et cliquez sur les **petits groupes de session de client** suivant les indications de l'image :

Étape 4. Le WLC étranger change alors l'état à L2 authentique remplit et envoie la réponse d'association au client.

> **Note**: L'authentification MAC étant activé, la réponse d'association n'est pas envoyée jusqu'à ce que ceci soit terminé.

```
*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
```

Étape 5 : L'étranger initie alors le procédé de transfert à l'ancre. C'est vu le transfert de debug mobility sorti :

```
*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
```

Étape 6. Vous pouvez voir que le client entre dans l'état de PASSAGE sur le WLC étranger. L'état correct du client peut maintenant être vu seulement sur l'ancre. Voici un extrait de la sortie de show client detail collectée de l'étranger (seulement les informations pertinentes sont affichées) :

```
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
```

Étape 7. Le contrôleur étranger initie une demande de transfert avec l'ancre. Vous pouvez maintenant voir les messages de transfert ci-dessous :

```
*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
```

Étape 8. Le contrôleur d'ancre déplace alors le client à l'état exigé par DHCP. Une fois que le client obtient une adresse IP, le contrôleur continue à transformer et déplacer le client en état exigé par webauth central. Vous pouvez voir la même chose dans la sortie de show client detail collectée sur l'ancre :

```
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
```

Étape 9. Le WLC étranger commence simultanément le processus de comptabilité une fois qu'il entre le client dans l'état de passage. Il envoie le message de début de comptabilité à 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: La comptabilité doit seulement être configurée sur le WLC étranger.

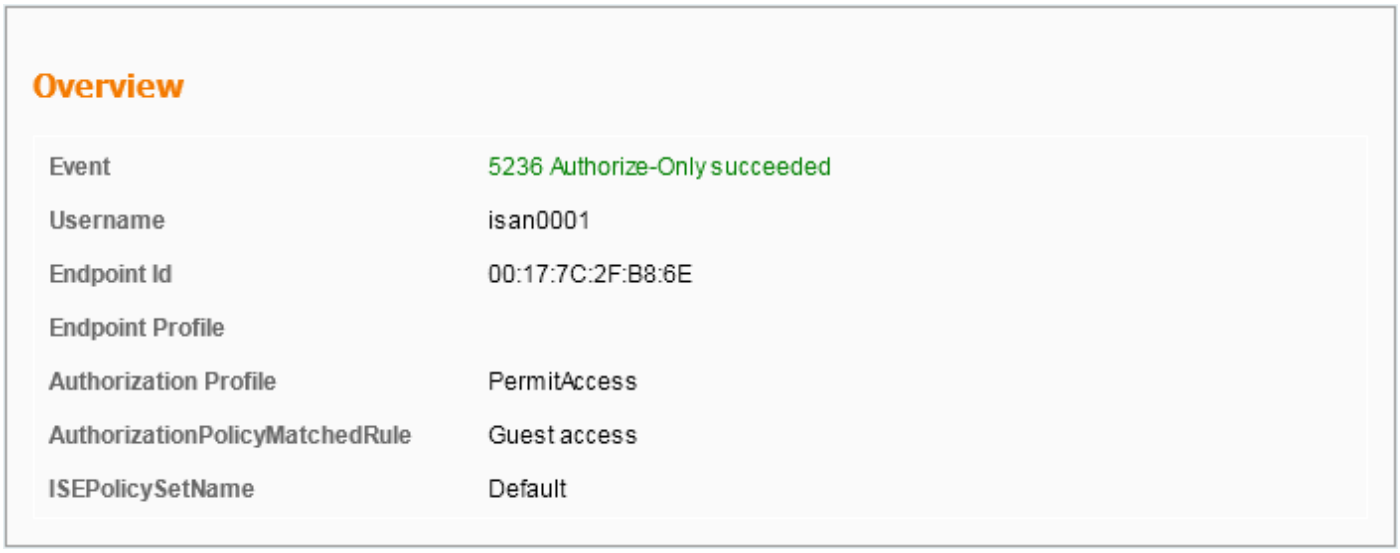
Étape 10. L'utilisateur initie alors le Web-auth réorientent le processus en écrivant un URL dans le navigateur. Vous pouvez voir que l'approprié met au point sur le contrôleur d'ancre :

```
*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
```

Étape 11. Nous pouvons également voir que la pièce d'authentification dans le processus de webauth est manipulée au WLC étranger et pas à l'ancre. Vous pouvez voir la même chose dans les sorties de debug aaa sur l'étranger :

```
*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)
```

Les mêmes peuvent être vérifiés sur ISE suivant les indications de l'image :



Étape 12. Ces informations sont passées sur l'ancre WLC. Cette prise de contact n'est pas clairement visible dans met au point et vous pouvez faire ceci par l'ancre qui applique une stratégie de transfert de courrier comme affiché ici :

```
*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.
```

La meilleure manière de vérifier que l'authentification est complète est de vérifier les logins passés ISE et de collecter la sortie du show client detail sur le contrôleur qui devrait afficher le client dans l'état de **PASSAGE** comme affiché ici :

```
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
```

Un autre important contrôle est le fait que l'ancre envoie un Protocole ARP (Address Resolution Protocol) gratuit après l'authentification réussie :

```
*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
```

D'ici le client est libre pour envoyer tous les types de trafic qui est expédié par le contrôleur d'ancre.

Écoulement central de Webauth quand le client obtient déconnecté

Quand une entrée de client doit être retirée du WLC ou dû à un délai d'attente de session/inactif ou quand nous retirons manuellement le client du WLC, ces étapes ont lieu :

WLC étranger envoie un message de De-authentifier au client et le programme pour la suppression :

```
*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
```

Il envoie alors un message de comptabilité d'arrêt de rayon pour informer le serveur ISE que la session d'authentification client a fini :

```
*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)
```

Il envoie également un message de transfert de mobilité à l'ancre WLC pour l'informer pour terminer la session de client. Ceci peut être vu dans la mobilité met au point sur l'ancre 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)
```

Compte de client interrompu sur ISE

ISE a la capacité d'interrompre un compte utilisateur d'invité qui signale le WLC pour terminer la session de client. C'est utile pour les administrateurs qui n'ont pas besoin de vérifier au lequel WLC le client est connecté et de terminer simplement la session. Vous pouvez maintenant voir ce qui se produit quand le compte utilisateur d'invité est interrompu/expiré sur ISE :

Le serveur ISE envoie une modification de message d'autorisation au contrôleur étranger qui indique que la connexion client doit être enlevée. Ceci peut être vu dans les sorties de débogage :

```
*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
```

WLC étranger envoie alors un message de De-authentifier au client :

```
*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)
```

Il envoie également un message d'arrêt de comptabilité au serveur de comptabilité pour finir la session d'authentification client de son côté :

```
*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)
```

Un message de transfert est également envoyé à l'ancre WLC pour terminer la session de client. Vous pouvez voir ceci sur l'ancre 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
```

Dépannez Webauth central dans l'installation d'ancre d'invité

Maintenant allons voir un regarder certains des problèmes courants vus quand vous utilisez CWA et ce qui peut être fait pour le réparer.

Le client du scénario 1. coincé dans l'état de DÉBUT et n'obtient pas l'adresse IP

Dans un scénario central de webauth puisque l'authentification MAC est activée, des réponses d'association sont envoyées après qu'une authentification MAC soit terminée. Dans ce cas, s'il y a une panne de communication entre le WLC et le serveur de rayon ou il y a un misconfig sur le serveur de rayon qui le fait envoyer des Access-anomalies, vous pouvez voir le client coincé dans une association pour faire une boucle où elle obtient à plusieurs reprises une anomalie d'association. Il y a également une occasion que le client obtient exclu aussi bien si l'exclusion de client est activée.

L'accessibilité de serveur de rayon peut être vérifiée avec la commande de **rayon d'AAA de test** qui est disponible en code 8.2 et en haut.

Le lien ci-dessous de référence affiche comment utiliser ceci :
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212473-verify-radius-server-connectivity-with-t.html

Le client du scénario 2. ne peut pas obtenir l'adresse IP

Il y a quelques raisons pour lesquelles un client peut pour obtenir une adresse IP dans une installation d'ancre d'invité CWA.

- **Le config SSID sur l'ancre et étranger ne s'assortit pas**

Il est idéal d'avoir le config SSID mêmes entre l'ancre et les WLC étrangers. Certains des aspects pour lesquels un contrôle strict est fait sont config de la Sécurité L2/L3, config DHCP et des paramètres de priorité d'AAA. Au cas où ce ne serait pas identique, un transfert à l'ancre échoue et vous pouvez voir que ces messages dans l'ancre met au point :

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

Afin d'atténuer ceci, vous devez s'assurer que le config SSID est la même ancre et étranger.

- **Le tunnel de mobilité entre l'ancre et les WLC étrangers sont réduit/s'agitant**

Tout le trafic de client est introduit le tunnel de données de mobilité qui utilise le protocole 97 IP. Si le tunnel de mobilité n'est pas vers le haut de puis vous pouvez voir que le transfert ne se termine pas et le client n'entre pas dans l'état de PASSAGE sur l'étranger. L'état de tunnel de mobilité doit afficher en tant que et peut être vu sous des **groupes de >Mobility de Gestion de >Mobility de contrôleur** suivant les indications de l'image.

S'il y a seulement un contrôleur tracé en tant que membre (étranger ou ancre), alors vous pouvez également vérifier les statistiques globales de mobilité sous le **>Statistics de moniteur > les statistiques de mobilité.**

- **Réorientez l'ACL non configuré sur l'ancre ou les contrôleurs étrangers :**

Quand le nom de l'ACL de réorientation envoyé par le serveur de rayon n'apparie pas ce qui est configuré sur le WLC étranger, alors quoique l'authentification MAC soit terminée, le client est rejeté et ne poursuit pas pour faire le DHCP. Il n'est pas obligatoire de configurer les différentes règles d'ACL car le trafic de client est terminé sur l'ancre. Tant que il y a un ACL créé avec le même nom que l'ACL de réorientation, le client est remis hors fonction à l'ancre. Les besoins d'ancre d'avoir le nom et les règles d'ACL configurés correctement pour que le client se déplace au webauth ont exigé l'état.

Le client du scénario 3. n'obtient pas réorienté à la page Web

Il y a de nouveau quelques différentes raisons pour lesquelles une page de webauth peut pour obtenir affiché. Certaines des questions latérales communes WLC sont couvertes ici :

- **Questions de serveur DNS**

Les questions d'accessibilité/misconfig de serveur DNS sont l'une des raisons les plus communes pour lesquelles les clients n'obtiennent pas réorienté. Il peut également être difficile d'attraper ceci car il n'apparaît dans aucun log WLC ou met au point. Les besoins de l'utilisateur de vérifier si le config de serveur DNS poussé du serveur DHCP est correct et s'il soit accessible du client sans fil. Une consultation simple de DN du client non-travaillant est le moyen le plus simple de vérifier ceci.

- **Passerelle par défaut inaccessible quand vous utilisez le serveur DHCP interne sur l'ancre :**

Quand vous utilisez les serveurs DHCP internes, il est important de s'assurer que le config de passerelle par défaut est correct et le VLAN est permis sur le switchport qui se connecte à l'ancre WLC. Sinon, le client obtient une adresse IP, mais il ne pourra pas accéder à n'importe quoi. Vous pouvez vérifier la table ARP sur le client pour l'adresse MAC de la passerelle. C'est un moyen

rapide de vérifier la Connectivité L2 à la passerelle et cela il est accessible.