Comprendre Et Dépanner L'Authentification Web Centrale (CWA) Dans La Configuration De L'Ancrage Invité

Contenu

Introduction

Ce document décrit le fonctionnement du webauth central dans une configuration d'ancrage invité et certains des problèmes courants observés dans un réseau de production et comment ils peuvent être corrigés.

Conditions préalables

Conditions requises

Cisco recommande que vous connaissiez la configuration du webauth central sur le contrôleur de réseau local sans fil (WLC).

Ce document fournit les étapes relatives 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

Components Used

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

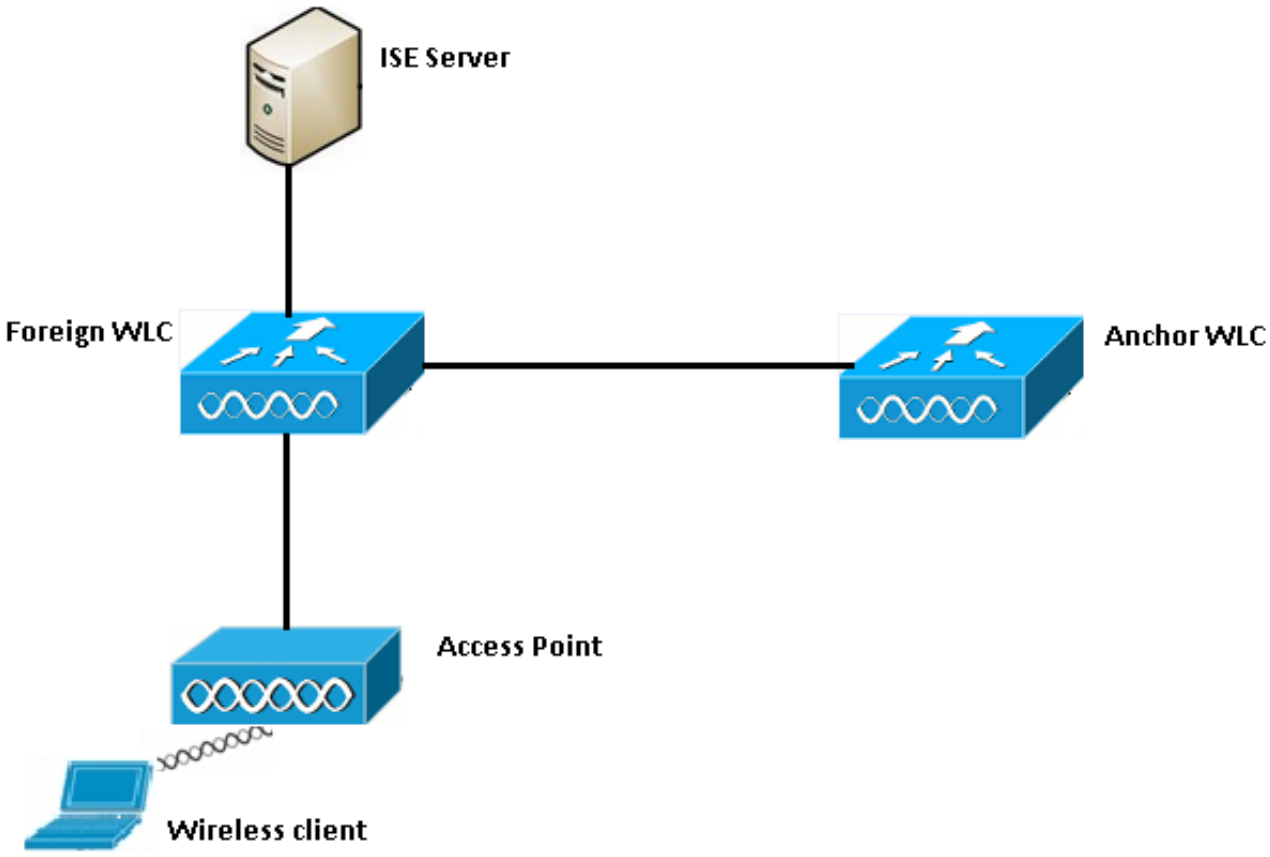
- WLC 5508 exécutant la version 7.6
- Identity Services Engine (ISE) version 1.4

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes

Flux de base

Cette section présente le flux de travail de base du webauth central dans une configuration d'ancrage invité, comme illustré dans l'image :



Étape 1. Le client démarre la connexion lorsqu'il envoie une demande d'association.

Étape 2. Le WLC commence le processus d'authentification MAC lorsqu'il envoie une demande d'authentification au serveur ISE configuré.

Étape 3. En fonction de la stratégie d'autorisation configurée sur ISE, le message Access-Accept est renvoyé au WLC avec les entrées de l'URL de redirection et de la liste de contrôle d'accès (ACL) de redirection.

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

Étape 5. Ces informations sont transmises par le WLC étranger au WLC d'ancrage dans les messages de transfert de mobilité. Vous devez vous assurer que les listes de contrôle d'accès de redirection sont configurées à la fois sur l'ancrage et sur les WLC étrangers.

Étape 6. À cette étape, le client passe à l'état Exécuter sur le WLC étranger.

Étape 7. Une fois que le client lance l'authentification Web avec une URL dans le navigateur, l'ancrage démarre le processus de redirection.

Étape 8. Une fois le client authentifié, il passe à l'état **RUN** sur le WLC d'ancrage.

Flot Webauth central pour tentative de connexion client réussie

Vous pouvez maintenant analyser le flux de base décrit ci-dessus en détail lorsque vous passez en revue les débogages. Ces débogages ont été collectés à la fois sur le point d'ancrage et sur le WLC étranger pour vous aider dans 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 informations sont utilisées 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 le processus de connexion lorsqu'il envoie une demande d'association. Ceci est visible 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 LAN sans fil (WLAN) est mappé pour l'authentification MAC et déplace le client vers l'état **AAA en attente**. Il commence également le processus d'authentification lorsqu'il envoie une demande d'authentification à ISE :

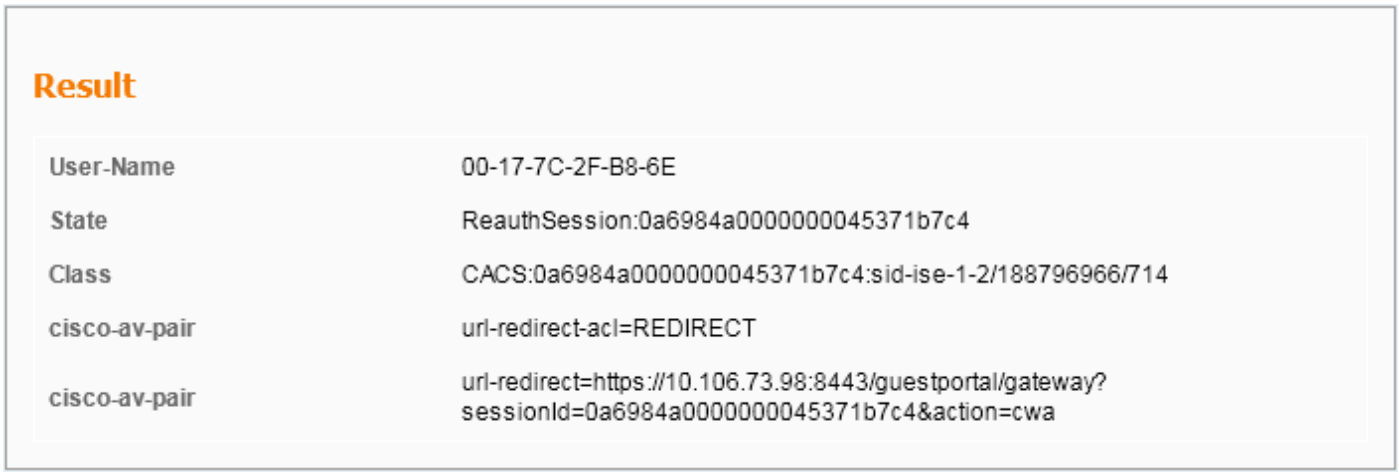
```
*apfMsConnTask_6: May 08 12:10:35.898: 00:17:7c:2f:b8:6e apfProcessAssocReq (apf_80211.c:8221)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Idle to AAA Pending
*aaaQueueReader: May 08 12:10:35.898: AuthenticationRequest: 0x2b6bf574

*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 de l'authentification MAC est configuré et retourne l'URL de redirection et la liste de contrôle d'accès après l'authentification MAC. Vous pouvez voir ces paramètres envoyés dans 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 dans les journaux ISE. Accédez à **Opérations >Authentifications** et cliquez sur **Détails de session client** comme indiqué dans l'image :



Étape 4. Le WLC étranger modifie ensuite l'état en auth L2 terminé et envoie la réponse d'association au client.

> **Note**: Lorsque l'authentification MAC est activée, la réponse d'association n'est pas envoyée tant que ce n'est pas 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 lance ensuite le processus de remise à l'ancre. Ceci est vu dans la sortie de transfert de mobilité de débogage :

```
*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 passe à l'état EXÉCUTION sur le WLC étranger. L'état correct du client ne peut désormais être vu que sur l'ancrage. Voici un extrait du résultat de la commande show client detail collecté à partir de l'étranger (seules 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 lance une demande de transfert avec l'ancrage. 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'ancrage déplace ensuite le client à l'état DHCP requis. Une fois que le client a obtenu une adresse IP, le contrôleur continue à traiter et à déplacer le client dans l'état requis du webauth central. Vous pouvez voir la même chose dans la sortie show client detail collectée sur l'ancrage :

```
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 démarre simultanément le processus de comptabilité une fois qu'il place le client dans l'état d'exécution. Il envoie un message de début de comptabilisation 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 uniquement être configurée sur le WLC étranger.

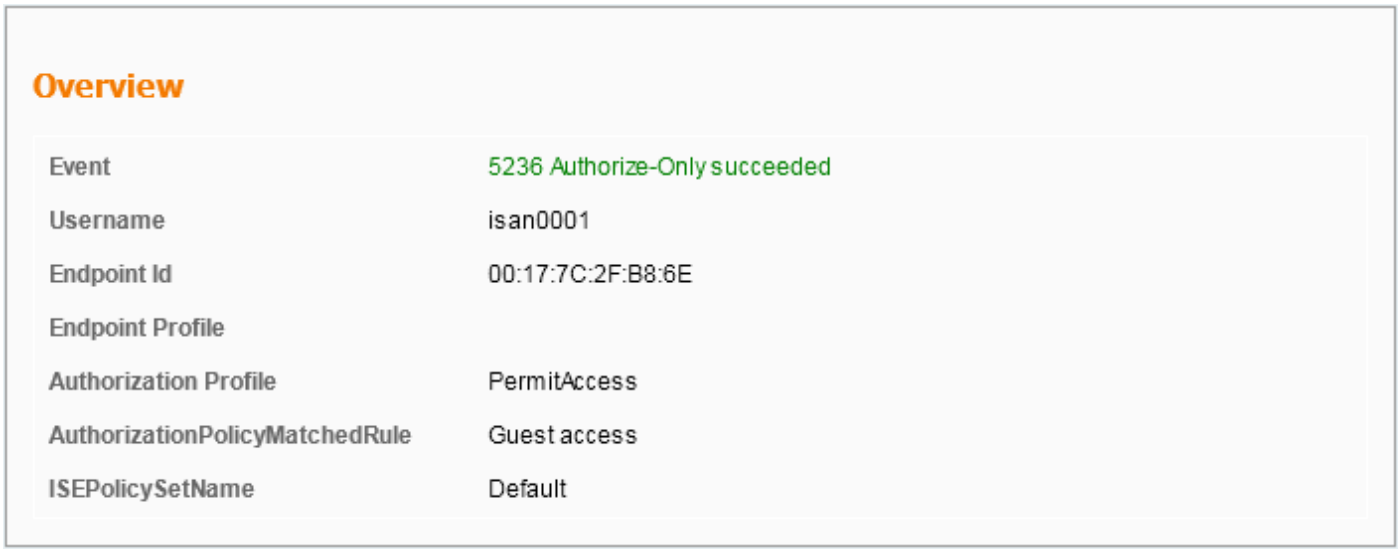
Étape 10. L'utilisateur lance ensuite le processus de redirection d'authentification Web en entrant une URL dans le navigateur. Vous pouvez voir les débogages appropriés sur le contrôleur d'ancrage :

```
*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 partie authentification dans le processus webauth est gérée au niveau du WLC étranger et non à l'ancrage. Vous pouvez voir la même chose dans les sorties de débogage 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)
```

Il est possible de vérifier la même chose sur ISE comme le montre l'image :



Étape 12. Ces informations sont transmises au WLC d'ancrage. Cette connexion n'est pas clairement visible dans les débogages et vous pouvez le distinguer par l'ancrage qui applique une politique de transfert de publication comme indiqué 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 façon de vérifier que l'authentification est complète est de vérifier les journaux passés sur ISE et de collecter la sortie de show client detail sur le contrôleur qui devrait afficher le client dans l'état **RUN** comme indiqué 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
```

Une autre vérification importante est le fait que l'ancrage envoie un protocole de résolution d'adresse (ARP) gratuit après une 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
```

Àpartir de là, le client est libre d'envoyer tous les types de trafic qui sont transférés par le contrôleur d'ancrage.

Flux Webauth central lorsque le client est déconnecté

Lorsqu'une entrée client doit être supprimée du WLC soit en raison d'un délai d'inactivité/session, soit lorsque nous supprimons manuellement le client du WLC, ces étapes se produisent :

Le WLC étranger envoie un message de désauthentification au client et le planifie pour 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 ensuite un message radius stop accounting pour informer le serveur ISE que la session d'authentification du client est terminée :

```
*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 au WLC d'ancrage pour l'informer de mettre fin à la session du client. Ceci peut être vu dans les débogages de mobilité sur le WLC d'ancrage :

```
*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 client suspendu sur ISE

ISE peut suspendre un compte d'utilisateur invité, ce qui indique au WLC de mettre fin à la session du client. Ceci est utile pour les administrateurs qui n'ont pas besoin de vérifier à quel WLC le client est connecté et de simplement mettre fin à la session. Vous pouvez maintenant voir ce qui se passe lorsque le compte d'utilisateur invité est suspendu/expiré sur ISE :

Le serveur ISE envoie un message de modification d'autorisation au contrôleur étranger qui indique que la connexion du client doit être supprimée. Ceci est visible 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
```

Le WLC étranger envoie ensuite un message de déauthentification 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 mettre fin à la session d'authentification du 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 au WLC d'ancrage pour mettre fin à la session du client. Vous pouvez voir ceci sur le WLC d'ancrage :

```
*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
```

Dépannage de l'authentification Web centralisée dans la configuration de l'ancrage invité

Examinons maintenant quelques-uns des problèmes courants rencontrés lors de l'utilisation de CWA et ce qui peut être fait pour les résoudre.

Scénario 1. Client bloqué dans l'état START et ne reçoit pas d'adresse IP

Dans un scénario de webauth central, puisque l'authentification MAC est activée, les réponses d'association sont envoyées après l'authentification MAC terminée. Dans ce cas, s'il y a une défaillance de communication entre le WLC et le serveur radius ou s'il y a une erreur de configuration sur le serveur radius qui l'entraîne à envoyer des refus d'accès, vous pouvez voir le client coincé dans une boucle d'association où il obtient à plusieurs reprises un rejet d'association. Il est également possible que le client soit également exclu si l'exclusion du client est activée.

L'accessibilité du serveur radius peut être vérifiée avec la commande **test aaa radius** disponible dans le code 8.2 et les versions ultérieures.

Le lien de référence ci-dessous indique 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

Scénario 2. Le client ne peut pas obtenir d'adresse IP

Il y a quelques raisons pour lesquelles un client ne parvient pas à obtenir une adresse IP dans une configuration d'ancrage invité CWA.

- **La configuration SSID sur l'ancre et l'étrangère ne correspond pas**

Il est idéal d'avoir une configuration SSID identique entre l'ancrage et les WLC étrangers. Certains des aspects pour lesquels une vérification stricte est effectuée sont la configuration de sécurité L2/L3, la configuration DHCP et les paramètres de remplacement AAA. Dans le cas contraire, une

remise à l'ancre échoue et vous pouvez voir ces messages dans les débogages de l'ancre :

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

Afin d'atténuer cela, vous devez vous assurer que la configuration SSID est la même ancrage et étrangère.

- **Le tunnel de mobilité entre l'ancre et les WLC étrangers est arrêté/clignotant**

Tout le trafic client est envoyé dans un tunnel de données de mobilité qui utilise le protocole IP 97. Si le tunnel de mobilité n'est pas actif, vous pouvez voir que la remise n'est pas terminée et que le client ne passe pas à l'état EXÉCUTÉ sur l'étranger. L'état du tunnel de mobilité doit s'afficher **UP** et peut être vu sous **Controller >Mobility Management >Mobility Groups** comme illustré dans l'image.

S'il n'y a qu'un seul contrôleur mappé en tant que membre (étranger ou ancre), vous pouvez également vérifier les statistiques de mobilité globale sous **Surveillance > Statistiques > Statistiques de mobilité.**

- **Rediriger la liste de contrôle d'accès non configurée sur l'ancre ou les contrôleurs étrangers :**

Lorsque le nom de la liste de contrôle d'accès de redirection envoyée par le serveur radius ne correspond pas à ce qui est configuré sur le WLC étranger, alors même que l'authentification MAC est terminée, le client est rejeté et ne continue pas à faire DHCP. Il n'est pas obligatoire de configurer les règles de liste de contrôle d'accès individuelles lorsque le trafic client est terminé sur l'ancre. Tant qu'une liste de contrôle d'accès est créée avec le même nom que la liste de contrôle d'accès de redirection, le client est transmis à l'ancre. Le nom et les règles de la liste de contrôle d'accès doivent être configurés correctement pour que le client passe à l'état requis pour l'authentification Web.

Scénario 3. Le client n'est pas redirigé vers la page Web

Il y a à nouveau quelques raisons différentes pour lesquelles une page de webauth peut ne pas s'afficher. Voici quelques-uns des problèmes courants du côté du WLC :

- **Problèmes de serveur DNS**

Les problèmes d'accessibilité/de configuration incorrecte du serveur DNS sont l'une des raisons les plus courantes pour lesquelles les clients ne parviennent pas à être redirigés. Cela peut également être difficile à saisir car il n'apparaît dans aucun journal ou débogage de WLC. L'utilisateur doit vérifier si la configuration du serveur DNS envoyée à partir du serveur DHCP est correcte et si elle est accessible à partir du client sans fil. Une simple recherche DNS à partir du client qui ne fonctionne pas est le moyen le plus simple de vérifier ceci.

- **Passerelle par défaut inaccessible lorsque vous utilisez un serveur DHCP interne sur ancre :**

Lorsque vous utilisez des serveurs DHCP internes, il est important de s'assurer que la configuration de la passerelle par défaut est correcte et que le VLAN est autorisé sur le port de commutateur qui se connecte au WLC d'ancrage. Si ce n'est pas le cas, le client obtient une adresse IP, mais il ne pourra accéder à rien. Vous pouvez vérifier l'adresse MAC de la passerelle dans la table ARP du client. Il s’agit d’un moyen rapide de vérifier la connectivité de couche 2 à la passerelle et de vérifier qu’elle est accessible.