Comprendere E Risolvere I Problemi Relativi All'Autenticazione Web Centrale (CWA) Nella Configurazione Dell'Ancoraggio Guest

Sommario

Introduzione

Questo documento descrive il funzionamento di webauth centrale in una configurazione di ancoraggio guest e alcuni dei problemi comuni rilevati in una rete di produzione e come possono essere risolti.

Prerequisiti

Requisiti

Cisco consiglia di essere a conoscenza di come configurare l'autenticazione Web centrale sul controller WLC.

In questo documento viene descritto come configurare l'autenticazione Web centrale: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

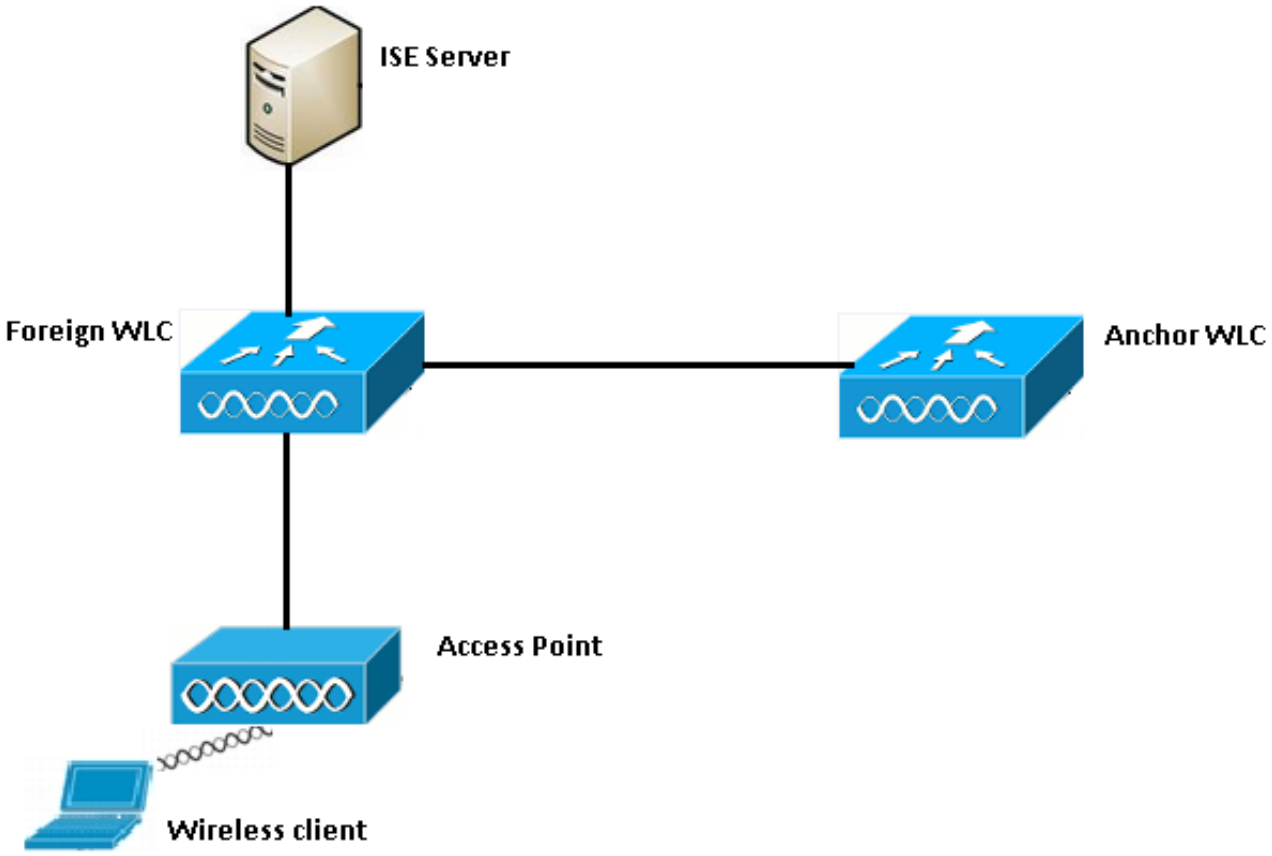
- WLC 5508 con versione 7.6
- Identity Services Engine (ISE) con versione 1.4

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi

Flusso di base

Questa sezione mostra il flusso di lavoro di base di webauth centrale in un'impostazione di ancoraggio guest, come mostrato nell'immagine:



Passaggio 1. Il client avvia la connessione quando invia una richiesta di associazione.

Passaggio 2. WLC avvia il processo di autenticazione MAC quando invia una richiesta di autenticazione al server ISE configurato.

Passaggio 3. In base alla policy di autorizzazione configurata su ISE, il messaggio Access-Accept viene inviato nuovamente al WLC con l'URL di reindirizzamento e le voci redirect Access Control List (ACL).

Passaggio 4. Il WLC esterno invia quindi una risposta dell'associazione al client.

Passaggio 5. Queste informazioni vengono passate dal WLC esterno al WLC principale nei messaggi di handoff per la mobilità. È necessario verificare che gli ACL di reindirizzamento siano configurati sia sull'ancoraggio sia sui WLC esterni.

Passaggio 6. In questa fase, il client passa allo stato di esecuzione sul WLC esterno.

Passaggio 7. Dopo che il client ha avviato l'autenticazione Web con un URL nel browser,

l'ancoraggio avvia il processo di reindirizzamento.

Passaggio 8. Dopo aver autenticato correttamente il client, questo passa allo stato **RUN** sul WLC di ancoraggio.

Flusso Webauth centrale per tentativo di connessione client riuscito

Èora possibile analizzare in dettaglio il flusso di base descritto in precedenza durante l'esecuzione dei debug. Questi debug sono stati raccolti sia sull'ancora che sul WLC esterno per facilitare l'analisi:

```
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
```

Questi dettagli sono utilizzati qui:

```
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
```

Passaggio 1. Il client avvia il processo di connessione quando invia una richiesta di associazione. Questa condizione viene rilevata sul controller esterno:

```
*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
```

Passaggio 2. Il WLC rileva che la LAN wireless (WLAN) è mappata per l'autenticazione MAC e sposta il client nello stato **AAA in sospeso**. Avvia inoltre il processo di autenticazione quando invia una richiesta di autenticazione ad ISE:

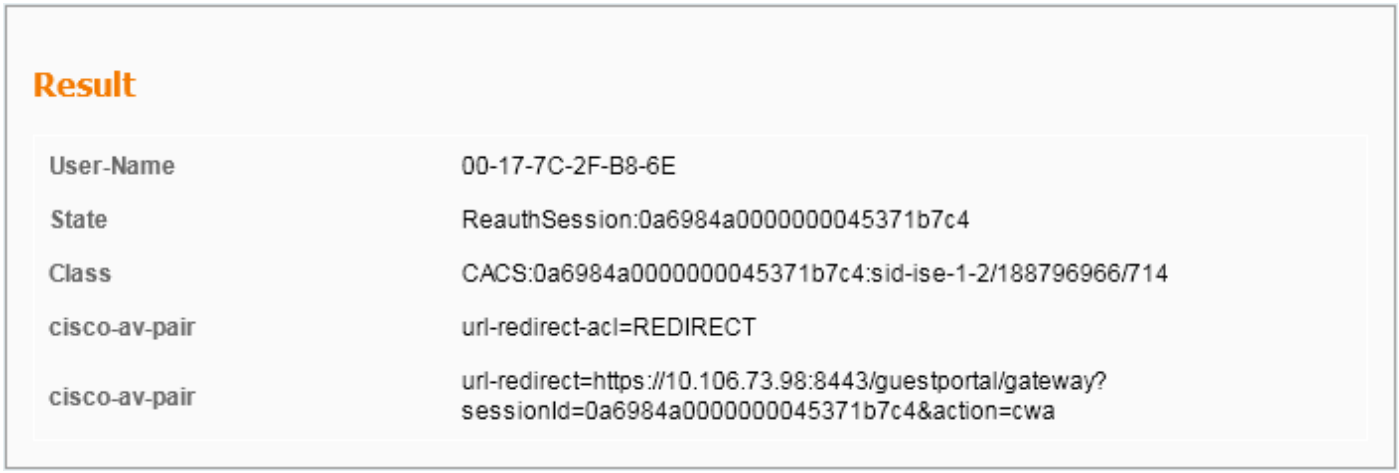
```
*apfMsConnTask_6: May 08 12:10:35.898: 00:17:7c:2f:b8:6e apfProcessAssocReq (apf_80211.c:8221)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Idle to AAA Pending
*aaaQueueReader: May 08 12:10:35.898: AuthenticationRequest: 0x2b6bf574

*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
```

Passaggio 3. Su ISE, il bypass dell'autenticazione MAC è configurato e restituisce l'URL di reindirizzamento e l'ACL dopo l'autenticazione MAC. Nella risposta di autorizzazione è possibile visualizzare i parametri seguenti:

```
*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)
```

Le stesse informazioni possono essere visualizzate nei log ISE. Passare a **Operazioni >Autenticazioni** e fare clic su **Dettagli sessione client**, come mostrato nell'immagine:



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

Passaggio 4. Il WLC esterno modifica quindi lo stato in Autenticazione L2 completata e invia la risposta dell'associazione al client.

> **Nota:** Se l'autenticazione MAC è abilitata, la risposta dell'associazione non viene inviata fino al completamento dell'operazione.

```
*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
```

Passaggio 5: Il dispositivo esterno avvia quindi il processo di passaggio all'ancora. Questo è l'output del comando debug mobility handoff:

```
*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
```

Passaggio 6. È possibile verificare che il client passa nello stato RUN sul WLC esterno. Lo stato corretto del client può ora essere visualizzato solo sull'ancoraggio. Di seguito è riportato un frammento dell'output del comando show client detail raccolto dall'esterno (vengono visualizzate solo le informazioni rilevanti):

```
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
```

Passaggio 7. Il controller esterno avvia una richiesta di handoff con l'ancoraggio. Di seguito sono riportati i messaggi di handoff:

```
*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
```

Passaggio 8. Il controller di ancoraggio passa quindi il client allo stato DHCP richiesto. Una volta che il client ottiene un indirizzo IP, il controller continua a elaborare e spostare il client nello stato webauth richiesto centrale. Lo stesso risultato si può verificare nell'output di visualizzazione dei dettagli client raccolti sull'ancoraggio:

```
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
```

Passaggio 9. Il WLC esterno avvia contemporaneamente il processo di contabilità quando sposta il client in stato di esecuzione. Invia ad ISE il messaggio di inizio contabilità:

```
*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)
```

Nota: È necessario configurare l'accounting solo sul WLC esterno.

Passaggio 10. L'utente avvia quindi il processo di reindirizzamento con autenticazione Web immettendo un URL nel browser. È possibile visualizzare i relativi debug sul controller di ancoraggio:

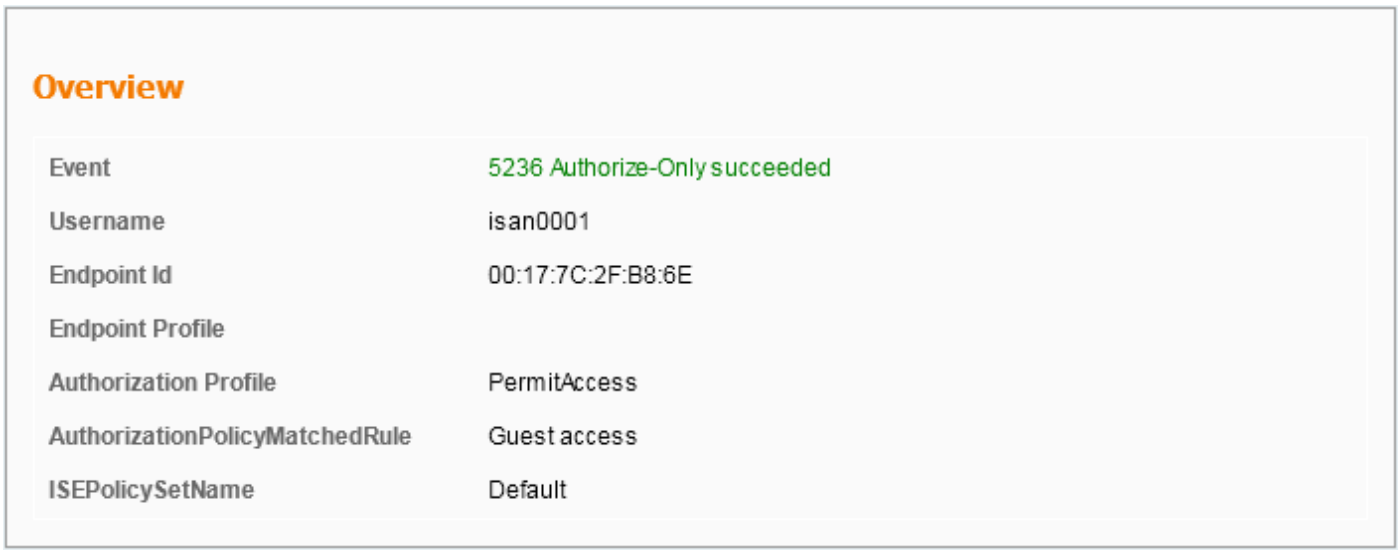
```
*webauthRedirect: May 08 05:53:05.927: 0:17:7c:2f:b8:6e- received connection
*webauthRedirect: May 08 05:53:05.928: captive-bypass detection disabled, Not checking for wispr
in HTTP GET, client mac=0:17:7c:2f:b8:6e
*webauthRedirect: May 08 05:53:05.928: 0:17:7c:2f:b8:6e- Preparing redirect URL according 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
```

Passaggio 11. È inoltre possibile verificare che la parte di autenticazione nel processo webauth viene gestita nel WLC esterno e non nell'ancoraggio. Lo stesso risultato si può verificare negli output del comando debug AAA sull'host esterno:

```
*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)
```

Lo stesso può essere verificato su ISE come mostrato nell'immagine:



Passaggio 12. Queste informazioni vengono passate al WLC di ancoraggio. Questo handshake non è chiaramente visibile nei debug ed è possibile renderlo visibile dall'ancoraggio che applica un criterio di handoff post, come mostrato di seguito:

```
*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.
```

Il modo migliore per verificare che l'autenticazione sia completa è verificare i log passati su ISE e raccogliere l'output del comando show client detail sul controller. Il client deve essere visualizzato nello stato **RUN**, come mostrato di seguito:

```
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'altra importante verifica è rappresentata dal fatto che, dopo l'autenticazione, l'ancoraggio invia gratuitamente un protocollo ARP (Address Resolution Protocol):

```
*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
```

Da qui il client è libero di inviare tutti i tipi di traffico che vengono inoltrati dal controller di ancoraggio.

Flusso autenticazione Web centrale alla disconnessione del client

Quando è necessario rimuovere una voce del client dal WLC a causa di un timeout di sessione/inattività o quando si rimuove manualmente il client dal WLC, vengono eseguiti i seguenti passaggi:

Il WLC esterno invia un messaggio di disautenticazione al client e lo pianifica per l'eliminazione:

```
*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
```

Quindi, invia un messaggio radius stop accounting per informare il server ISE che la sessione di autenticazione client è terminata:

```
*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)
```

Inoltre, invia un messaggio di handoff relativo alla mobilità al WLC di ancoraggio per informarlo di terminare la sessione client. Questa condizione può essere rilevata nei debug sulla mobilità sul WLC di ancoraggio:

```
*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)
```

Account client sospeso ad ISE

ISE ha la capacità di sospendere un account utente guest che indica al WLC di terminare la sessione client. Ciò è utile per gli amministratori che non hanno bisogno di controllare a quale WLC è connesso il client e semplicemente terminare la sessione. Ecco cosa succede quando l'account utente guest viene sospeso/scaduto ad ISE:

Il server ISE invia un messaggio di modifica dell'autorizzazione al controller esterno per comunicargli che la connessione del client deve essere rimossa. Questa condizione può essere rilevata negli output del comando 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
```

Il WLC esterno invia quindi un messaggio di disautenticazione al 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)
```

Invia inoltre un messaggio di interruzione dell'accounting al server di accounting per terminare la sessione di autenticazione client sul lato corrispondente:

```
*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)
```

Viene inoltre inviato un messaggio di handoff al WLC di ancoraggio per terminare la sessione client. Sul WLC di ancoraggio è possibile visualizzare quanto segue:

```
*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
```

Risoluzione dei problemi di Central Webauth nella configurazione dell'ancoraggio guest

Esaminiamo ora alcuni dei problemi più comuni riscontrati durante l'utilizzo di CWA e vengono descritte le possibili soluzioni.

Scenario 1. Client bloccato nello stato START e senza indirizzo IP

In uno scenario di autenticazione Web centrale, poiché l'autenticazione MAC è abilitata, le risposte di associazione vengono inviate dopo il completamento dell'autenticazione MAC. In questo caso, se si verifica un errore di comunicazione tra il WLC e il server radius o una configurazione errata sul server radius che causa l'invio di richieste di accesso rifiutate, è possibile vedere il client bloccato in un loop di associazione in cui riceve ripetutamente un rifiuto di associazione. Esiste anche la possibilità che il client venga escluso se l'esclusione del client è attivata.

La raggiungibilità del server radius può essere verificata con il comando **test aaa radius** disponibile in codice 8.2 e versioni successive.

Il link di riferimento riportato di seguito illustra come utilizzare questa funzionalità:
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212473-verify-radius-server-connectivity-with-t.html

Scenario 2. Il client non è in grado di ottenere l'indirizzo IP

Esistono alcuni motivi per cui un client non riesce a ottenere un indirizzo IP in una configurazione dell'ancoraggio guest di CWA.

- **La configurazione SSID sull'ancoraggio e quella esterna non corrispondono**

Èideale avere la stessa configurazione SSID tra l'ancora e i WLC esterni. Alcuni degli aspetti per i quali viene eseguito un controllo rigoroso sono la configurazione della sicurezza L2/L3, la configurazione DHCP e i parametri di override AAA. In caso contrario, si verifica un errore di handoff dell'ancoraggio e nei debug dell'ancoraggio vengono visualizzati questi messaggi:

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

Per evitare questo problema, è necessario verificare che la configurazione SSID sia dello stesso ancoraggio e esterna.

- **Tunnel di mobilità tra le porte di ancoraggio e i WLC esterni non funzionanti**

Tutto il traffico del client viene inviato nel tunnel dati di mobilità che utilizza il protocollo IP 97. Se il tunnel di mobilità non è attivo, è possibile notare che il passaggio non viene completato e il client non passa allo stato di esecuzione sull'esterno. Lo stato del tunnel per la mobilità deve essere visualizzato come **UP** e può essere visualizzato in **Controller > Mobility Management > Mobility Groups** (Controller > Gestione mobilità > Gruppi di mobilità), come mostrato nell'immagine.

Se esiste un solo controller mappato come membro (straniero o ancora), è possibile controllare le statistiche globali sulla mobilità in **Monitoraggio > Statistiche > Statistiche mobilità.**

- **ACL di reindirizzamento non configurato sull'ancoraggio o sui controller esterni:**

Quando il nome dell'ACL di reindirizzamento inviato dal server radius non corrisponde a quello configurato sul WLC esterno, anche se l'autenticazione MAC è stata completata, il client viene rifiutato e non continua a eseguire DHCP. Non è obbligatorio configurare le singole regole ACL perché il traffico del client viene terminato sull'ancoraggio. Se è stato creato un ACL con lo stesso nome dell'ACL di reindirizzamento, il client viene consegnato all'ancoraggio. Affinché il client passi allo stato richiesto webauth, è necessario che il nome ACL e le regole dell'ancoraggio siano configurati correttamente.

Scenario 3. Il client non viene reindirizzato alla pagina Web

Esistono ancora alcuni motivi diversi per cui una pagina webauth non viene visualizzata. Di seguito sono illustrati alcuni dei problemi più comuni relativi al lato WLC:

- **Problemi del server DNS**

I problemi di raggiungibilità/configurazione errata del server DNS sono uno dei motivi più comuni per cui i client non vengono reindirizzati. Questa condizione può anche essere difficile da rilevare in quanto non viene visualizzata in alcun registro WLC o debug. L'utente deve verificare se la configurazione del server DNS sottoposta a push dal server DHCP è corretta e se è raggiungibile dal client wireless. Una semplice ricerca DNS dal client non funzionante è il modo più semplice

per verificare questa condizione.

- **Gateway predefinito non raggiungibile quando si usa il server DHCP interno sull'ancoraggio:**

Quando si usano server DHCP interni, è importante verificare che la configurazione del gateway predefinito sia corretta e che la VLAN sia consentita sulla porta dello switch che si connette al WLC di ancoraggio. In caso contrario, il client ottiene un indirizzo IP, ma non sarà in grado di accedere a nulla. È possibile controllare la tabella ARP sul client per l'indirizzo MAC del gateway. È un modo rapido per verificare la connettività L2 al gateway e che sia raggiungibile.