瞭解訪客錨點設定中的中央Web驗證(CWA)並疑難排解

目錄

簡介

本文說明中央webauth在訪客錨點設定中如何運作，以及生產網路中常見的一些問題，以及如何解決這些問題。

必要條件

需求

思科建議您瞭解如何配置無線LAN控制器(WLC)上的中央webauth。

本文提供中央webauth的設定步驟：
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

採用元件

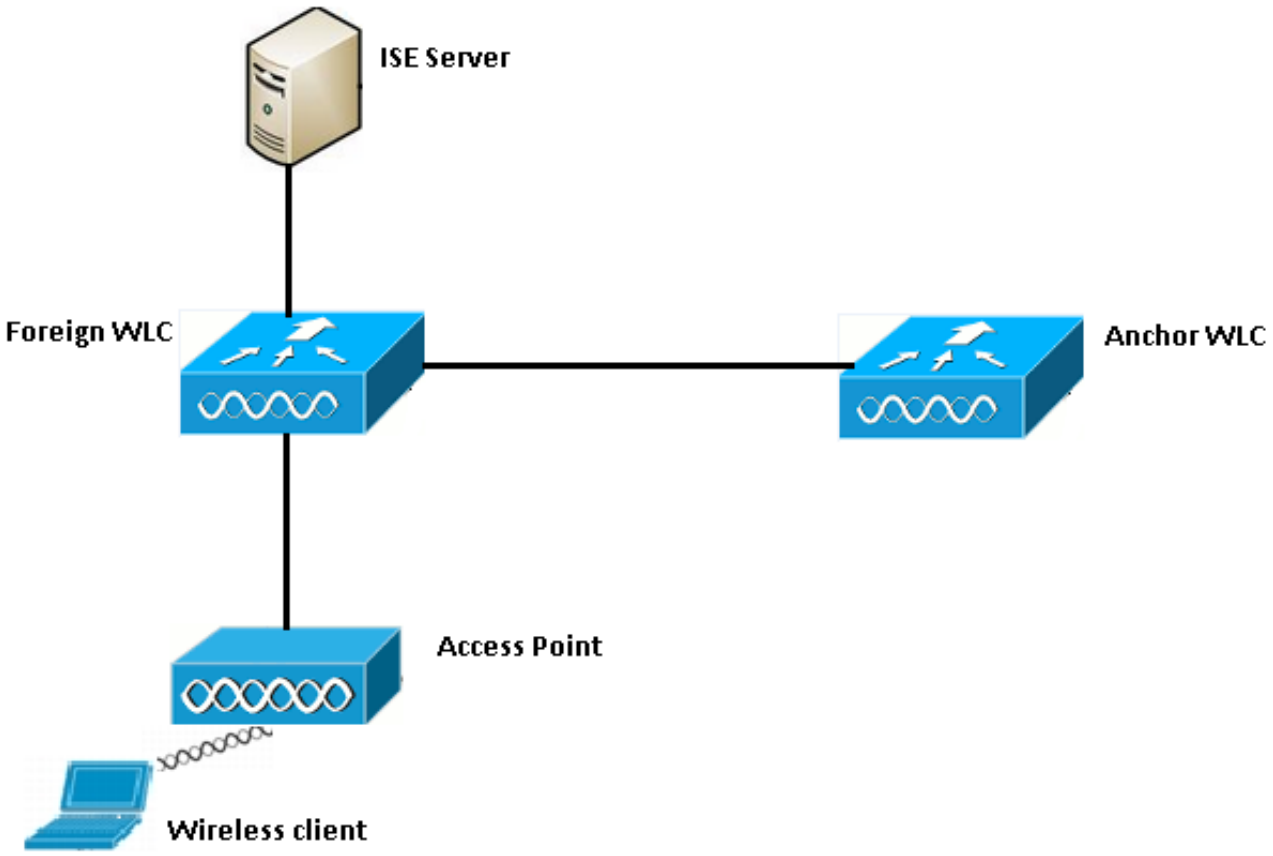
本文中的資訊係根據以下軟體和硬體版本：

- 執行版本7.6的WLC 5508
- 執行版本1.4的身分識別服務引擎(ISE)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響

基本流程

本節顯示訪客錨點設定中中央webauth的基本工作流程，如下圖所示：



步驟1.客戶端在傳送關聯請求時啟動連線。

步驟2. WLC將身份驗證請求傳送到所配置的ISE伺服器時，會開始MAC身份驗證過程。

步驟3.根據在ISE上配置的授權策略，使用重定向URL和重定向訪問控制清單(ACL)條目將訪問接受消息傳送回WLC。

步驟4.外部WLC隨後將關聯響應傳送到使用者端。

步驟5.在行動化交接訊息中，此資訊由外部WLC傳遞至錨點WLC。您需要確保在錨點和外部WLC上皆設定重新導向ACL。

步驟6.在這個階段，使用者端在外部WLC上進入執行狀態。

步驟7.使用者端使用瀏覽器中的URL發起web-auth後，錨點會啟動重新導向程式。

步驟8。使用者端成功通過驗證後，錨點WLC上的使用者端會進入**RUN**狀態。

成功的客戶端連線嘗試的中央Webauth流

現在，您可以在調試過程中詳細分析上述基本流程。已在錨點和外部WLC上收集到以下調試，以協助您進行分析：

```
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
```

此處使用以下詳細資訊：

```
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
```

步驟1.客戶端在傳送關聯請求時開始連線過程。在外部控制器上可看到以下情況：

```
*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
```

步驟2. WLC看到已對映無線LAN(WLAN)以進行MAC驗證，並將使用者端移至**AAA待定**狀態。當向ISE傳送身份驗證請求時，也會開始身份驗證過程：

```
*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
```

步驟3.在ISE上配置MAC身份驗證繞行，並在MAC身份驗證後返回重定向URL和ACL。您可以在授權響應中看到這些引數：

```
*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)
```

您可以在ISE日誌下看到相同的資訊。導覽至**操作>驗證**，然後按一下Client session details，如下圖所示：

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

步驟4.外部WLC接著將狀態變更為L2 auth complete，並將關聯回應傳送到使用者端。

附註：啟用MAC身份驗證後，在完成此操作之前不會傳送關聯響應。

```
*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
```

第5步：然後，外部發起到錨點的切換過程。調試移動性切換輸出如下所示：

```
*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
```

步驟6。您可以看到使用者端在外部WLC上進入RUN狀態。現在，只能在錨點上看到客戶端的正確狀態。以下是從外部收集的show client detail輸出的片段（僅顯示相關資訊）：

```
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
```

步驟7.外部控制器向錨點發起切換請求。現在您可以看到以下切換消息：

```
*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
```

步驟8.然後，錨點控制器將客戶端移動到DHCP所需狀態。使用者端取得IP位址後，控制器會繼續處理使用者端，並將使用者端移入中央webauth需要狀態。在錨點上收集的show client detail輸出中可看到相同的內容：

```
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
```

步驟9.外部WLC在使使用者端進入執行狀態後同時開始記賬流程。向ISE傳送記帳開始消息：

```
*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)
```

附註：只需要在外部WLC上配置記帳。

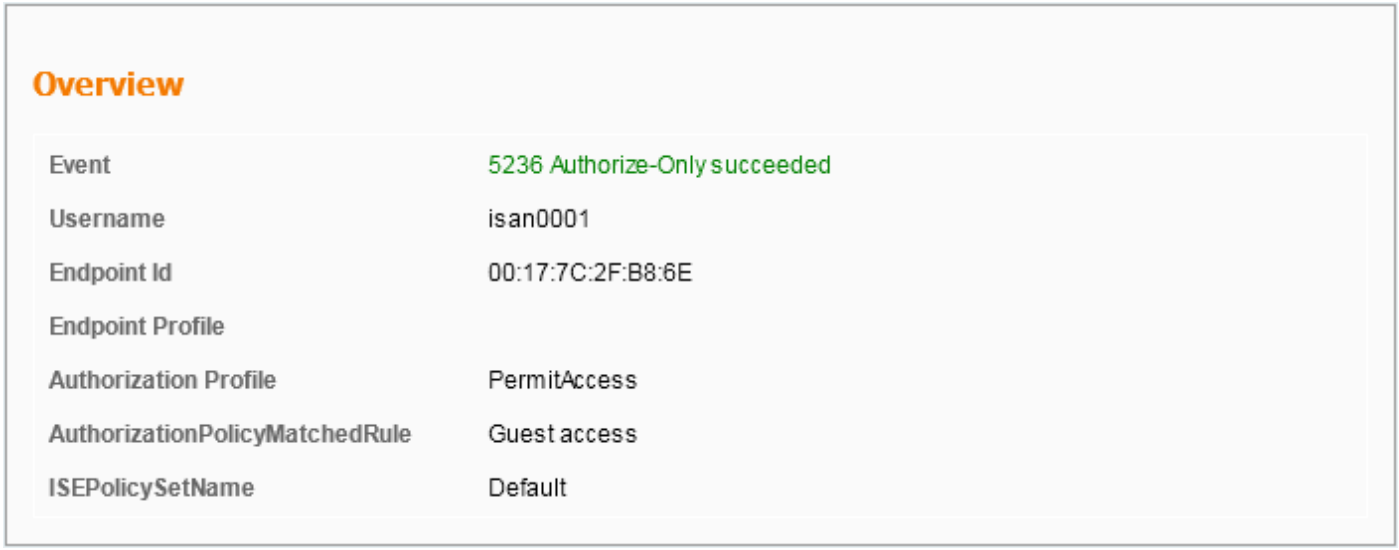
步驟10.使用者接著在瀏覽器中輸入URL以啟動web-auth重新導向程式。您可以在錨點控制器上看到相關調試：

```
*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
```

步驟11。我們也會看到webauth進程中的驗證部分是在外部WLC處理，而不是在錨點處理。在foreign上的debug AAA輸出中可看到相同的內容：

```
*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)
```

在ISE上也可驗證相同情況，如下圖所示：



步驟12.此資訊會傳遞至錨點WLC。此握手在調試中不可見，您可以由應用後切換策略的錨點進行驗證，如下所示：

```
*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.
```

驗證身份驗證是否完整的最佳方式是驗證ISE上傳遞的日誌並收集控制器上show client detail的輸出，該輸出應顯示客戶端處於**RUN**狀態，如下所示：

```
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
```

另一個重要的檢查是錨點在成功驗證後傳送了無償位址解析通訊協定(ARP):

```
*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
```

從這裡開始，使用者端可以自由傳送所有型別的流量，這些流量由錨點控制器轉發出去。

客戶端斷開連線時的中央Webauth流

當由於作業階段/閒置逾時需要從WLC移除使用者端專案時，或我們手動從WLC移除使用者端時，會發生以下步驟：

外部WLC將取消驗證訊息傳送給使用者端，並安排其刪除作業：

```
*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
```

然後傳送radius stop記帳消息通知ISE伺服器客戶端身份驗證會話已結束：

```
*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)
```

它還向錨點WLC傳送移動性切換消息，以通知其終止客戶端會話。可以在錨點WLC上的行動化偵錯中看到這種情況：

```
*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)
```

ISE上的客戶端帳戶已掛起

ISE能夠掛起訪客使用者帳戶，該帳戶向WLC發出訊號以終止客戶端會話。這對於不需要檢查使用者端連線到哪個WLC且只需終止作業階段的管理員很有用。現在，您可以看到當訪客使用者帳戶在ISE上暫停/到期時會發生什麼情況：

ISE伺服器向外部控制器傳送授權更改消息，指示需要刪除客戶端連線。可以在偵錯輸出中看到這種情況：

```
*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
```

然後，外部WLC將取消驗證訊息傳送給使用者端：

```
*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)
```

它還會向記帳伺服器傳送記帳停止消息，以結束客戶端身份驗證會話：

```
*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)
```

切換消息也傳送到錨點WLC以終止客戶端會話。您可以在錨點WLC上看到以下內容：

```
*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
```

訪客錨點設定中的中央Webauth疑難排解

現在，讓我們看一下在使用CWA時看到的一些常見問題，以及可以做些什麼來解決它。

案例1.使用者端停滯在START狀態且未取得IP位址

在啟用MAC身份驗證後的中央webauth方案中，關聯響應在MAC身份驗證完成後傳送。在此案例中，如果WLC和radius伺服器之間發生通訊失敗，或radius伺服器上發生導致其傳送存取拒絕的錯誤組態，您就會看到使用者端停滯在關聯回圈中，重複獲得關聯拒絕。如果啟用了客戶端排除，也可能排除客戶端。

可以使用**test aaa radius**命令驗證radius伺服器的可達性，該命令在代碼8.2和更高版本中可用。

下面的參考連結顯示了如何使用此功能：
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212473-verify-radius-server-connectivity-with-t.html

案例2.使用者端無法取得IP位址

客戶端在CWA訪客錨點設定中無法獲取IP地址的原因有幾個。

- **錨點和外部SSID配置不匹配**

在錨點和外部WLC之間最好使SSID配置相同。進行嚴格檢查的一些方面是L2/L3安全配置、DHCP配置和AAA覆蓋引數。如果不相同，則向錨點的切換將失敗，您可以在錨點的調試中看到以下消息：

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

要緩解此問題，您需要確保SSID配置是相同的錨點和外部。

- **錨點和外部WLC之間的行動通道發生關閉/擺動**

所有客戶端流量都在使用IP協定97的移動資料隧道中傳送。如果移動隧道未啟動，則您會看到切換未完成，客戶端在外部未進入RUN狀態。行動通道狀態需顯示為**UP**，可在**Controller > Mobility Management > Mobility Groups**下看到，如下圖所示。

如果只有一個控制器對映為成員（外部或錨點），則還可以檢查**Monitor >Statistics > Mobility Statistics下的全域性移動統計資訊。**

- **未在錨點或外部控制器上配置重定向ACL:**

當radius伺服器傳送的重新導向ACL的名稱與外部WLC上設定的名稱不符時，則即使MAC驗證完成，使用者端也會遭到拒絕，且不會進行DHCP。由於客戶端流量在錨點上終止，因此不必配置單個ACL規則。只要使用與重新導向ACL相同的名稱建立的ACL，就會將客戶端傳遞給錨點。錨點需要正確配置ACL名稱和規則，客戶端才能進入webauth必需狀態。

案例3.使用者端沒有重新導向到網頁

同樣有幾個不同的原因會導致無法顯示webauth頁面。以下是關於一些常見的WLC端問題：

- **DNS伺服器問題**

DNS伺服器可達性/配置錯誤問題是客戶端無法重定向的最常見原因之一。這也很難擷取，因為它在任何WLC記錄或偵錯中都沒有顯示。使用者需要驗證從DHCP伺服器推送的DNS伺服器配置是否正確，以及是否可以從無線客戶端訪問。從非工作客戶端進行簡單的DNS查詢是檢查此情況的最簡單方法。

- **在錨點上使用內部DHCP伺服器時無法訪問預設網關：**

使用內部DHCP伺服器時，必須確保預設閘道組態正確無誤，且連線到錨點WLC的switchport上允許使用VLAN。如果沒有，則客戶端獲得IP地址，但無法訪問任何內容。您可以在客戶端的ARP表中查詢網關的MAC地址。這是一種快速檢驗到網關的L2連線以及它是否可到達的方法。