了解并且排除故障中央Web验证(CWA)在访客锚点设置

目录

简介

本文描述中央webauth如何在设置的访客锚点工作和在生产网络看到的某些常见问题，并且他们如何可以修复。

先决条件

要求

思科建议您有关于怎样的知识配置在无线局域网控制器(WLC)的中央webauth。

本文提供步骤关于中央webauth的配置：
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

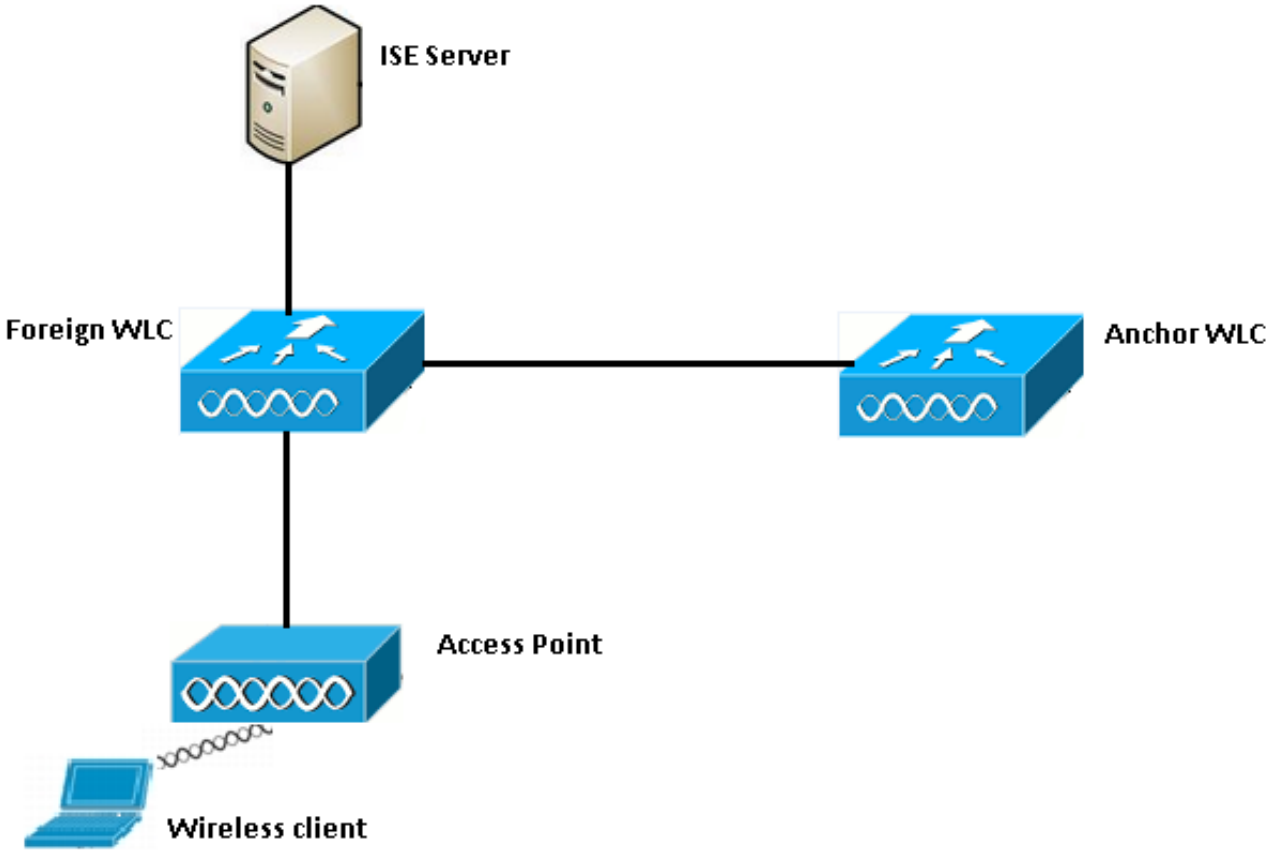
使用的组件

本文档中的信息基于以下软件和硬件版本：

- WLC 5508运行的版本7.6
- 身份服务引擎(ISE)运行版本1.4

基本流

如镜像所显示，此部分显示中央webauth基本工作流在访客锚点设置的：



步骤1.，当它发送关联申请时，客户端开始连接。

步骤2.，当发送认证请求到配置时的ISE服务器WLC开始MAC验证进程。

步骤3.基于在ISE配置的授权策略， Access-Accept消息被退还的对与重定向URL和重定向访问控制表(ACL)条目的WLC。

第四步：外国WLC然后发送对客户端的一关联答复。

第五步：此信息由对锚点WLC的外国WLC通过在移动性移交消息。您需要保证重定向ACL在锚点和外国WLC's配置。

步骤6.在此阶段，客户端搬入在外国WLC的运转状态。

步骤 7.一旦客户端启动与URL的web-auth在浏览器，锚点开始重定向过程。

步骤 8一旦客户端顺利地验证，客户端搬入在锚点WLC的运转状态。

成功的客户端连接尝试的中央Webauth流

当您通过调试时，您能当前分析详细描述的基本流以上。这些调试在锚点和外国WLC收集帮助与您的分析：

```
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
```

使用得这些详细信息这里：

```
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
```

步骤1:当它发送关联申请时，客户端开始连接进程。这在外国控制器被看到：

```
*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
```

第二步：WLC看到无线局域网(WLAN)为MAC验证被映射并且迁移客户端向**AAA待定**状态。当发送认证请求对ISE时，它也开始认证过程：

```
*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
```

第三步：在ISE， MAC验证旁路配置，并且在MAC验证以后返回重定向URL和ACL。您能看到在授权应答发送的这些参数：

```
*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)
```

您能看到同一信息在ISE日志下。如镜像所显示，导航对**操作>Authentications**并且单击**客户端会话详细信息**：

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

第四步：外国WLC然后更改状态对L2完整的验证并且发送对客户端的关联答复。

Note:当MAC验证启用，关联答复没有被发送，直到这完成。

```
*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
```

步骤 5：外国然后开始移交进程到锚点。这是看到输出的调试移动性移交：

```
*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
```

第六步：您能看到客户端搬入在外国WLC的运转状态。客户端的正确状态在锚点能当前仅被看到。这是从外国收集的显示客户端详细信息输出的片断(仅相关信息显示)：

```
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
```

步骤 7.外国控制器启动一移交请求用锚点。您能当前看到下面移交消息：

```
*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
```

步骤 8锚点控制器然后迁移客户端向DHCP要求的状态。一旦客户端获得IP地址，控制器继续处理和切换客户端到中央webauth要求的状态。您在锚点收集的显示客户端详细信息输出中能看到同样：

```
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
```

步骤 9一旦切换客户端到运转状态，外国WLC同时开始核算进程。它传送核算启动消息对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:认为在外国WLC只需要配置。

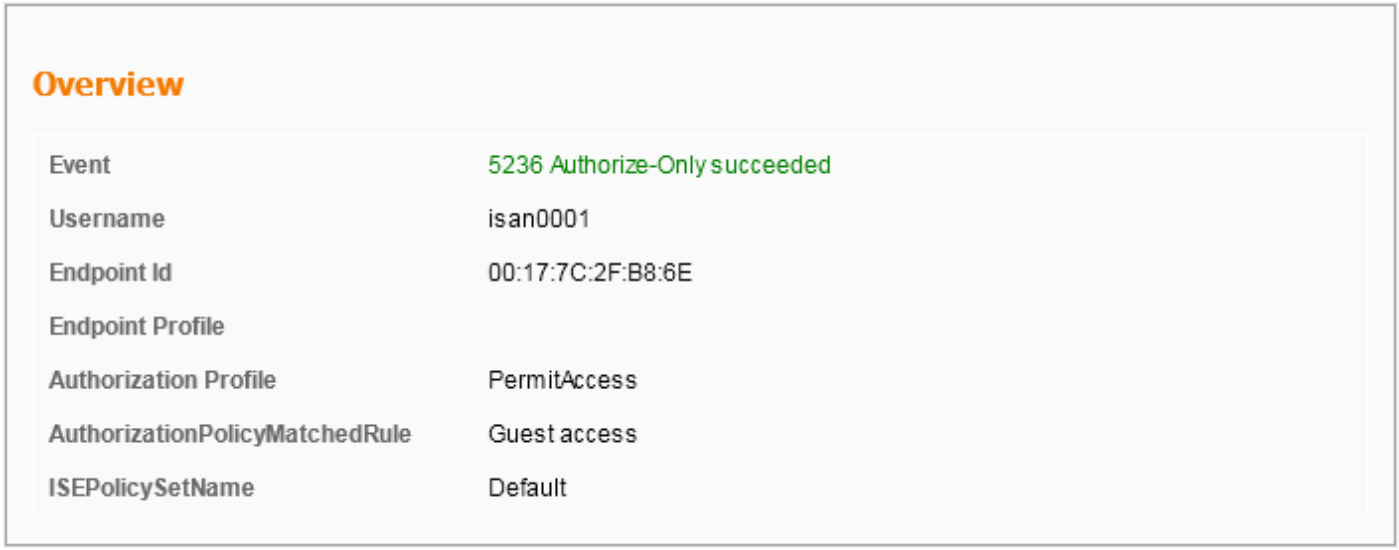
步骤 10用户通过输入在浏览器的URL然后开始web-auth重定向进程。您能看到在锚点控制器的相关调试：

```
*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
```

步骤 11我们能也看到webauth进程的验证零件被处理在外国WLC和不在锚点。您在外国的debug aaa输出中能看到同样：

```
*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)
```

如镜像所显示，同样在ISE可以验证：



步骤 12此信息通过在锚点WLC上。此握手不清楚地是可视在调试，并且您能由运用发表物移交策略如显示此处的锚点做此：

```
*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.
```

验证的最佳方法验证完成是验证合格注册ISE并且收集输出显示在控制器的客户端详细信息哪些应该显示运转状态的客户端如显示此处：

```
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
```

另一重要检查是事实锚点在成功认证以后发送无偿地址解析协议(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
```

从在这里由锚点控制器转发的客户端自由发送所有流量类型。

中央Webauth流，当客户端断开

当客户端条目需要从WLC删除或者由于会话/空闲超时时或者，当我们从WLC时手工删除客户端，这些步骤发生：

外国WLC传送DE验证信息给客户端并且安排它于删除：

```
*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
```

它然后传送radius终止核算信息通知ISE服务器客户端验证会话结束了：

```
*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)
```

它也传送移动性移交信息对锚点WLC通知它终止客户端会话。这在锚点WLC的移动性调试能被看到：

```
*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)
```

在ISE暂停的客户端帐户

ISE有能力暂停发信号WLC终止客户端会话的来宾用户用户帐号。这为不需要检查的管理员是有用的哪WLC客户端连接对和终止会话。您能当前看到发生了什么，当来宾用户用户帐号在ISE时被暂停/超时：

ISE服务器派遣授权消息的崔凡吉莱到表明的外国控制器客户端连接需要删除。这在debug输出中能被看到：

```
*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
```

外国WLC然后传送DE验证信息给客户端：

```
*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)
```

它也传送核算终止信息到记帐服务器结束在其侧的客户端验证会话：

```
*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)
```

移交信息也传送对锚点WLC终止客户端会话。您在锚点WLC能看到此：

```
*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
```

排除故障在访客锚点设置的中央Webauth

当前请让我们查看一下被看到的某些常见问题，当您使用CWA时，并且什么可以执行修复它。

在启动状态滞留的方案1.客户端，并且没获得IP地址

在一个中央webauth方案中，因为MAC验证启用，关联答复被发送，在MAC验证完成后。在这种情况下，如果有在WLC和RADIUS服务器之间的一个通信故障或者有在造成它发送访问拒绝的RADIUS服务器的一misconfig，您能看到在关联中滞留的客户端循环重复获得关联拒绝的地方。如果客户端排除启用，也有机会被排除的客户端获得。

RADIUS服务器可接通性可以用是可用的用代码8.2以上的**测验AAA RADIUS**命令验证。

下面的参考链路显示如何使用此：
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212473-verify-radius-server-connectivity-with-t.html

方案2.客户端无法获得IP地址

有一些个原因为什么客户端可以不能获得在CWA访客锚点设置的一个IP地址。

- **在锚点的SSID设置和外国不配比**

有SSID设置同样在锚点和外国WLC's之间是理想的。严格的检查是完成的某些方面是L2/L3安全设置、DHCP设置和AAA覆盖参数。万一这不是相同的，对锚点的一移交发生故障，并且您能看到在锚点调试的这些消息：

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

为了缓和此，您需要保证SSID设置同一个锚点和外国。

- **在锚点和外国WLC's之间的移动性通道下降/飘荡**

所有客户端的流量在移动性使用IP协议97的数据通道发送。如果移动性通道不是那么您能看到移交不完成，并且客户端不搬入在外国的运转状态。如镜像所显示，移动性隧道状态需要显示作为并且能被看到在**控制器>Mobility管理>Mobility组下。**

如果只有作为成员被映射的一个控制器(外国或锚点)，则您能也检查全局移动性统计信息在**箴言报>Statistics >移动性统计信息下。**

- **重定向在锚点或外国控制器没配置的ACL ：**

当RADIUS服务器发送的重定向ACL的名称不匹配时什么在外国WLC配置，然后，即使MAC验证完成，客户端拒绝和不继续执行DHCP。因为客户端的流量在锚点，终止配置个人ACL规则是不必须的。只要有ACL创建与名称和重定向ACL一样，客户端被递交到锚点。锚点需要有为了客户端和规则正确地配置的ACL名称能迁移向webauth要求的状态。

方案3.客户端不重新定向对网页

再有一些个不同的原因为什么webauth页可以不能获得显示。某些普通的WLC枝节问题报道此处：

- **DNS服务器问题**

DNS服务器可接通性/misconfig问题是多数常见原因之一客户端为什么不能重新定向。因为在任何WLC日志或调试，没出现这可以也是难捉住。用户需要验证，如果从DHCP服务器推送的DNS服务器设置正确，并且是否从无线客户端是可及的。从非工作的客户端的简单DNS查找是检查此的简便的方法。

- **不可得到的默认网关，当您使用在锚点的内部DHCP服务器：**

当您使用内部DHCP服务器时，请注意默认网关设置正确，并且连接对锚点WLC的VLAN在switchport允许。否则，客户端获得IP地址，但是不能访问任何东西。您能检查在客户端的ARP表网关的MAC地址。它是快速方式验证L2连接到网关，并且那可及的。