Zentrale Webauthentifizierung (CWA) bei Einrichtung eines Gastanschlusses verstehen und Fehler beheben

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie eine zentrale Webauth in einer Gastanker-Konfiguration funktioniert und wie einige der häufig auftretenden Probleme in einem Produktionsnetzwerk behoben werden können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse zur Konfiguration einer zentralen Webauth auf dem Wireless LAN Controller (WLC) verfügen.

Dieses Dokument enthält Schritte zur Konfiguration einer zentralen Webauth: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

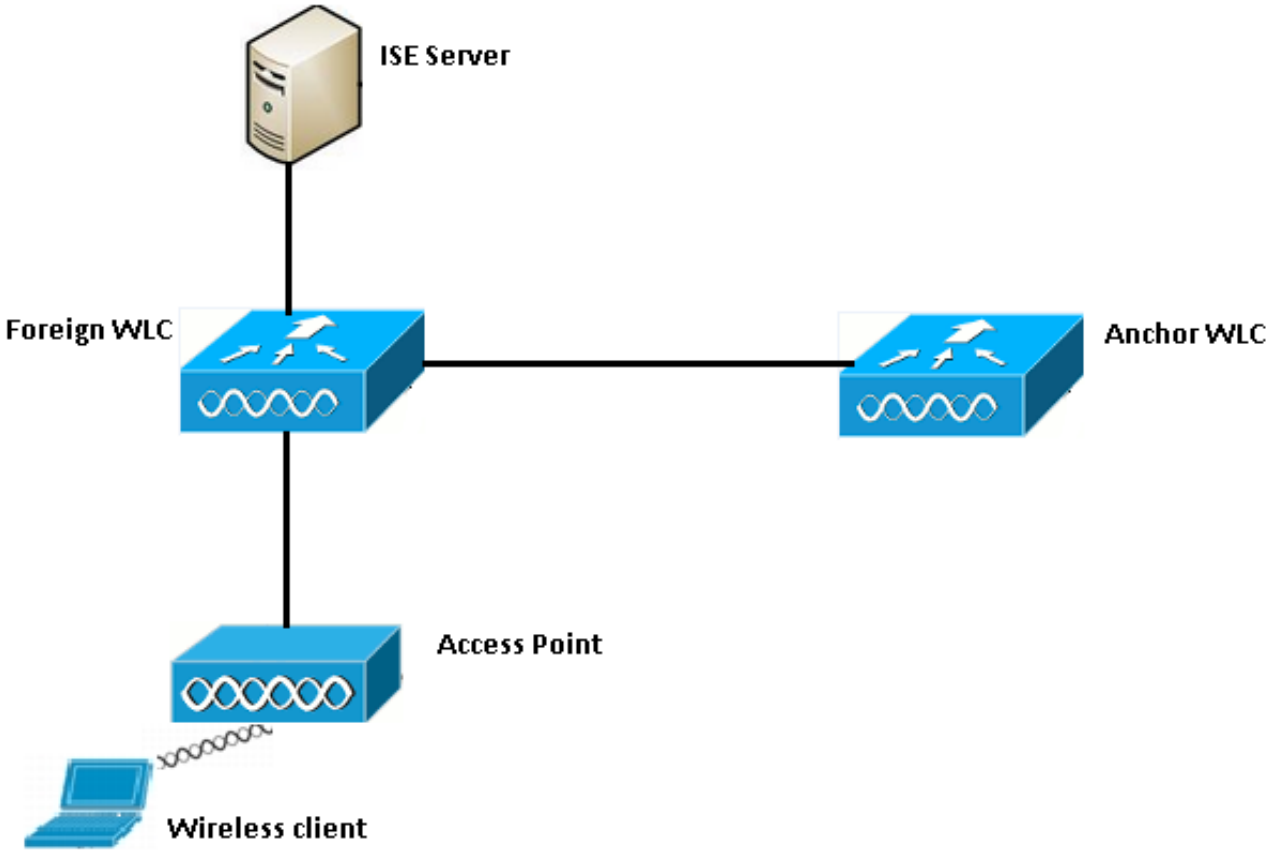
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- WLC 5508 mit Version 7.6
- Identity Services Engine (ISE) mit Version 1.4

Basisfluss

In diesem Abschnitt wird der grundlegende Workflow der zentralen Webauth-Funktion in einer Gastankereinrichtung wie im Bild gezeigt angezeigt:



Schritt 1: Der Client startet die Verbindung, wenn er eine Zuordnungsanfrage sendet.

Schritt 2: WLC startet den MAC-Authentifizierungsprozess, wenn eine Authentifizierungsanfrage an den konfigurierten ISE-Server gesendet wird.

Schritt 3: Basierend auf der auf der ISE konfigurierten Autorisierungsrichtlinie wird die Access-Accept-Nachricht mit der Umleitungs-URL an den WLC zurückgesendet und Zugriffskontrolllisten-Einträge umgeleitet.

Schritt 4: Der ausländische WLC sendet dann eine Assoziations-Antwort an den Client.

Schritt 5: Diese Informationen werden vom ausländischen WLC an den Anker-WLC in Mobility Handoff-Nachrichten weitergeleitet. Sie müssen sicherstellen, dass die Umleitungszugriffskontrolllisten sowohl für den Anker als auch für externe WLCs konfiguriert sind.

Schritt 6: In dieser Phase wechselt der Client auf dem ausländischen WLC in den Status "Ausführen".

Schritt 7: Sobald der Client die Webauthentifizierung mit einem URL im Browser initiiert hat, startet der Anker den Umleitungsprozess.

Schritt 8: Sobald der Client erfolgreich authentifiziert wurde, wechselt der Client auf dem Anker-

WLC in den **RUN**-Status.

Zentraler Webauth-Fluss für erfolgreichen Client-Verbindungsversuch

Sie können jetzt den oben beschriebenen grundlegenden Fluss detailliert analysieren, wenn Sie die Debugging-Vorgänge durchführen. Diese Debuggen wurden sowohl für den Anker als auch für den ausländischen WLC gesammelt, um die Analyse zu unterstützen:

```
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
```

Diese Details werden hier verwendet:

```
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
```

Schritt 1: Der Client startet den Verbindungsprozess, wenn er eine Zuordnungsanforderung sendet. Dies wird auf dem ausländischen Controller angezeigt:

```
*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
```

Schritt 2: Der WLC erkennt, dass das Wireless LAN (WLAN) der MAC-Authentifizierung zugeordnet ist, und verschiebt den Client in den **ausstehenden AAA**-Status. Er beginnt auch mit dem Authentifizierungsprozess, wenn er eine Authentifizierungsanfrage an die ISE sendet:

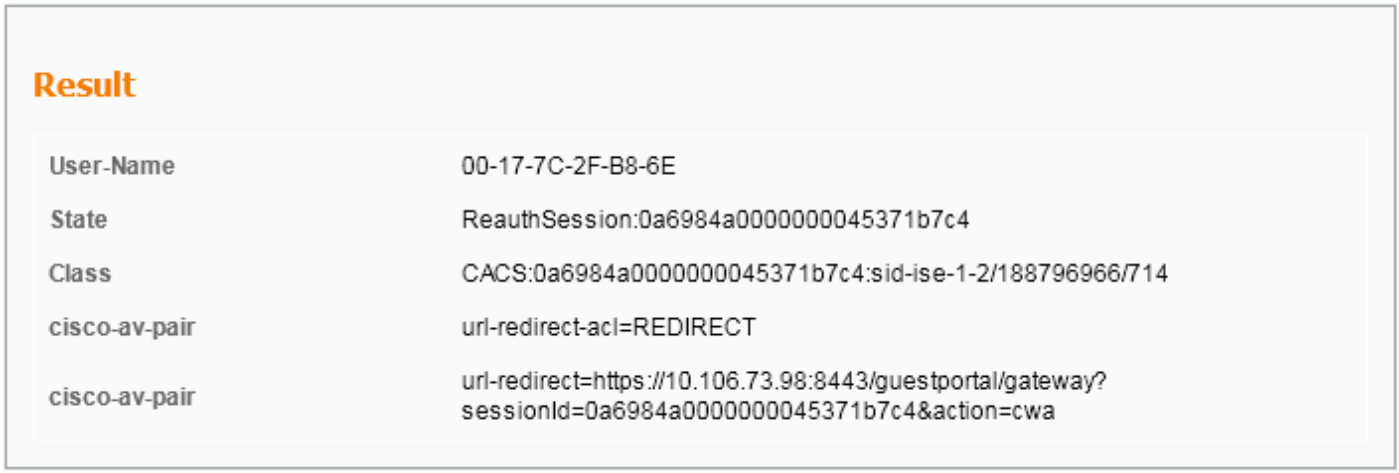
```
*apfMsConnTask_6: May 08 12:10:35.898: 00:17:7c:2f:b8:6e apfProcessAssocReq (apf_80211.c:8221)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Idle to AAA Pending
*aaaQueueReader: May 08 12:10:35.898: AuthenticationRequest: 0x2b6bf574

*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
```

Schritt 3: Auf der ISE wird eine Umgehung der MAC-Authentifizierung konfiguriert, und die Umleitungs-URL und die ACL werden nach der MAC-Authentifizierung zurückgegeben. Diese Parameter werden in der Autorisierungsantwort gesendet:

```
*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)
```

Sie können die gleichen Informationen unter den ISE-Protokollen sehen. Navigieren Sie zu **Operations >Authentications**, und klicken Sie auf **Client session details**, wie im Bild gezeigt:



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

Schritt 4: Der ausländische WLC ändert dann den Zustand in "L2-Authentifizierung abgeschlossen" und sendet die Zuordnungsantwort an den Client.

> **Hinweis**: Bei aktivierter MAC-Authentifizierung wird erst dann eine Zuordnungsantwort gesendet, wenn diese abgeschlossen ist.

```
*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
```

Schritt 5: Das Fremdwort initiiert dann den Übergabeverfahren an den Anker. Dies wird in der Ausgabe der Debug-Mobility-Handoff angezeigt:

```
*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
```

Schritt 6: Wie Sie sehen, wechselt der Client auf dem ausländischen WLC in den RUN-Status. Der richtige Client-Status kann jetzt nur noch auf dem Anker angezeigt werden. Hier ein Ausschnitt der Ausgabe der show client detail aus dem Ausland (nur relevante Informationen werden angezeigt):

```
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
```

Schritt 7: Der ausländische Controller initiiert eine Übergabeanfrage mit dem Anker. Die folgenden Übermittlungsmeldungen werden angezeigt:

```
*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
```

Schritt 8: Der Anker-Controller verschiebt den Client in den erforderlichen DHCP-Status. Sobald der Client eine IP-Adresse erhält, fährt der Controller mit der Verarbeitung fort und verschiebt den Client in den erforderlichen zentralen Webauth-Status. Das Gleiche wird in der Ausgabe der Clientdetails anzeigen angezeigt, die für den Anker erfasst wurde:

```
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
```

Schritt 9: Der ausländische WLC startet gleichzeitig den Accounting-Prozess, sobald er den Client in den Ausführungszustand versetzt. Es sendet die Startnachricht für die Rechnungslegung an die 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)
```

Hinweis: Die Buchhaltung muss nur auf dem ausländischen WLC konfiguriert werden.

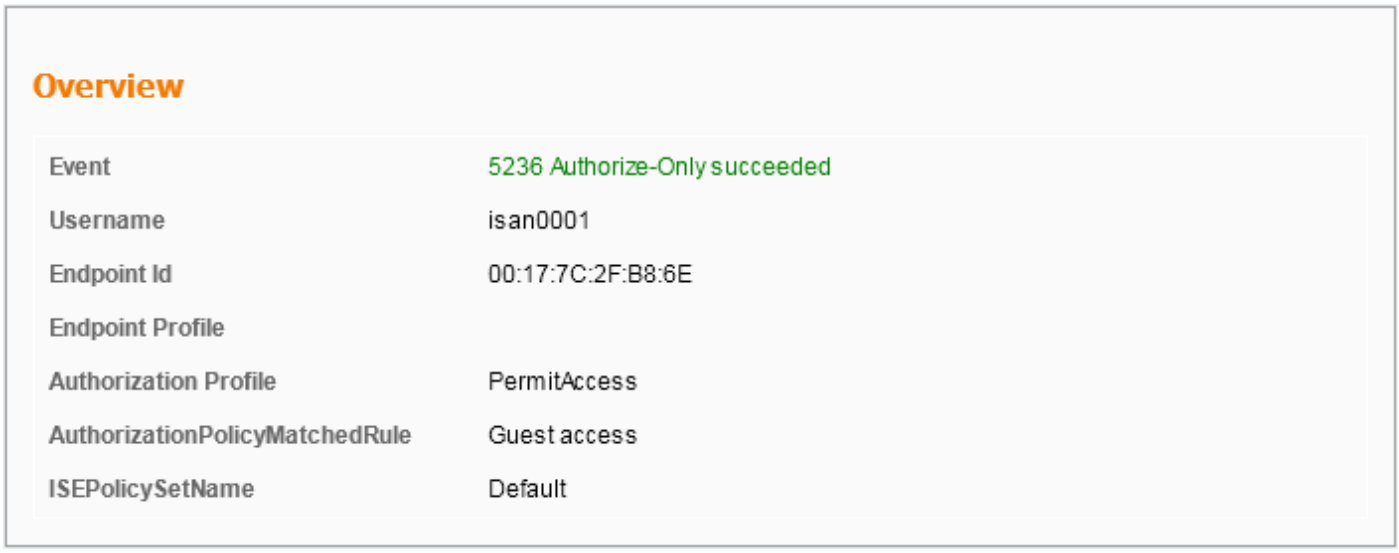
Schritt 10: Der Benutzer initiiert dann die Umleitung der Webauthentifizierung, indem er eine URL im Browser eingibt. Sie können die entsprechenden Debuggen auf dem Ankercontroller sehen:

```
*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
```

Schritt 11: Wir können auch sehen, dass der Authentifizierungsteil im Webauth-Prozess am ausländischen WLC und nicht am Anker behandelt wird. Das Gleiche wird in den Debug-AAA-Ausgaben für das Ausland angezeigt:

```
*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)
```

Auf der ISE kann dasselbe überprüft werden, wie im Bild gezeigt:



Schritt 12: Diese Informationen werden an den Anker WLC übergeben. Dieser Handshake ist im Debuggen nicht deutlich sichtbar, und Sie können dies durch den Anker hervorheben, der eine Richtlinie für die Postübergabe anwendet, wie hier gezeigt:

```
*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.
```

Die beste Methode, um sicherzustellen, dass die Authentifizierung abgeschlossen ist, besteht darin, die vergebenen Protokolle bei der ISE zu überprüfen und die Ausgabe von show client detail auf dem Controller zu erfassen. Diese sollte den Client im **RUN-**Zustand anzeigen, wie hier gezeigt:

```
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
```

Eine weitere wichtige Überprüfung besteht darin, dass der Anker nach erfolgreicher Authentifizierung ein kostenloses Address Resolution Protocol (ARP) sendet:

```
*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
```

Von hier aus kann der Client alle Arten von Datenverkehr senden, der vom Anker-Controller weitergeleitet wird.

Zentraler Webauth-Fluss, wenn der Client getrennt wird

Wenn ein Client-Eintrag aus dem WLC entfernt werden muss, entweder aufgrund einer Sitzungs-/Inaktivitäts-Zeitüberschreitung oder wenn der Client manuell aus dem WLC entfernt wird, werden folgende Schritte ausgeführt:

Ausländisches WLC sendet eine deauthentifizierte Nachricht an den Client und plant deren Löschung:

```
*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
```

Anschließend sendet er eine RADIUS Stopp Accounting-Meldung, um den ISE-Server darüber zu informieren, dass die Client-Authentifizierungssitzung beendet wurde:

```
*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)
```

Sie sendet außerdem eine Mobility Handoff-Nachricht an den Anker-WLC, um ihn zu informieren, dass er die Client-Sitzung beenden soll. Dies wird in den Mobility-Debugs auf dem Anker WLC angezeigt:

```
*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)
```

Client-Konto auf ISE ausgesetzt

Die ISE kann ein Gastbenutzerkonto aussetzen, das den WLC signalisiert, die Client-Sitzung zu beenden. Dies ist nützlich für Administratoren, die nicht überprüfen müssen, mit welchem WLC der Client verbunden ist, und die Sitzung einfach beenden müssen. Sie können jetzt sehen, was geschieht, wenn das Gastbenutzerkonto auf der ISE ausgesetzt/abgelaufen ist:

Der ISE-Server sendet eine Nachricht zur Autorisierungsänderung an den ausländischen Controller, die anzeigt, dass die Client-Verbindung entfernt werden muss. Dies wird in den Debug-Ausgaben angezeigt:

```
*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
```
Ausländisches WLC sendet dann eine de-authentication-Nachricht an den 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)
```
Es sendet außerdem eine Abrechnungs-Stoppmeldung an den Accounting-Server, um die Client-Authentifizierungssitzung auf seiner Seite zu beenden:

```
*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)
```
Eine Übergabemeldung wird auch an den Anker-WLC gesendet, um die Clientsitzung zu beenden. Sie können dies auf dem Anker WLC sehen:

```
*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
```

Fehlerbehebung Zentrale Webauth bei Einrichtung eines Gastanhangs

Sehen wir uns nun einige der häufigsten Probleme an, die bei der Verwendung von CWA aufgetreten sind, und wie diese behoben werden können.

Szenario 1. Client im START-Status steckt und IP-Adresse wird nicht abgerufen

In einem zentralen Webauth-Szenario werden Zuordnungsantworten nach Abschluss einer MAC-Authentifizierung gesendet, da die MAC-Authentifizierung aktiviert ist. Wenn in diesem Fall ein Kommunikationsfehler zwischen dem WLC und dem Radius-Server auftritt oder eine fehlerhafte Konfiguration auf dem Radius-Server das Senden von Access-Rejects bewirkt, wird der Client in einer Assoziationsschleife festgehalten, in der er wiederholt eine Ablehnung der Zuordnung erhält. Es besteht auch die Möglichkeit, dass der Client bei aktiviertem Clientausschluss ebenfalls ausgeschlossen wird.

Die Verfügbarkeit des Radius-Servers kann mit dem Befehl **test aaa radius** (**Testradius**) überprüft werden, der in Code 8.2 und höher verfügbar ist.

Der nachfolgende Referenzlink zeigt die Verwendung dieser Funktion:
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212473-verify-radius-server-connectivity-with-t.html

Szenario 2. Der Client kann die IP-Adresse nicht abrufen.

Es gibt einige Gründe, warum ein Client in einer CWA-Gastanker-Konfiguration keine IP-Adresse erhält.

- **Die SSID-Konfiguration für Anker und Fremd stimmt nicht überein.**

Ideal, wenn die SSID-Konfiguration zwischen dem Anker und den ausländischen WLCs identisch

ist. Zu den Aspekten, für die eine strenge Prüfung durchgeführt wird, gehören die L2/L3-Sicherheitskonfiguration, die DHCP-Konfiguration und die AAA-Überschreibungsparameter. Wenn dies nicht der Fall ist, schlägt die Übergabe an den Anker fehl, und die folgenden Meldungen werden im Ankerdebugger angezeigt:

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

Um dies zu verhindern, müssen Sie sicherstellen, dass die SSID-Konfiguration der gleiche Anker und Fremdkörper ist.

- **Mobility-Tunnel zwischen Anker- und ausländischen WLCs sind ausgefallen bzw. flattern.**

Der gesamte Client-Datenverkehr wird im Mobility Data Tunnel gesendet, der das IP-Protokoll 97 verwendet. Wenn der Mobility-Tunnel nicht aktiv ist, können Sie sehen, dass die Übergabe nicht abgeschlossen ist und der Client im Ausland nicht in den RUN-Status wechselt. Der Status des Mobility-Tunnels muss als **UP** angezeigt werden und kann unter **Controller >Mobility Management >Mobility Groups (Controller > Mobilitätsmanagement > Mobilitätsgruppen)** wie im Bild gezeigt angezeigt werden.

Wenn nur ein Controller als Mitglied zugeordnet ist (entweder extern oder Anker), können Sie die globalen Mobilitätsstatistiken auch unter **Monitor >Statistics > Mobility Statistics** überprüfen.

- **Die ACL für die Umleitung wird weder auf dem Anker noch auf den ausländischen Controllern konfiguriert:**

Wenn der Name der vom RADIUS-Server gesendeten Umleitungszugriffskontrollliste nicht mit dem auf dem ausländischen WLC konfigurierten Namen übereinstimmt, wird der Client abgelehnt, und DHCP wird nicht ausgeführt, obwohl die MAC-Authentifizierung abgeschlossen ist. Die Konfiguration der einzelnen ACL-Regeln ist nicht obligatorisch, da der Clientverkehr am Anker terminiert wird. Solange eine ACL mit demselben Namen wie die Umleitungszugriffskontrollliste erstellt wird, wird der Client an den Anker übergeben. Für den Anker müssen der ACL-Name und die Regeln korrekt konfiguriert sein, damit der Client in den erforderlichen Webauth-Status wechseln kann.

Szenario 3. Der Client wird nicht zur Webseite umgeleitet.

Es gibt wieder einige verschiedene Gründe, warum eine Webseite nicht angezeigt werden kann. Einige der häufigsten WLC-Probleme werden hier behandelt:

- **DNS-Serverprobleme**

Die Erreichbarkeit von DNS-Servern/Fehlkonfigurationen sind einer der häufigsten Gründe, warum Clients nicht umgeleitet werden. Dies kann auch schwer zu erfassen sein, da es nicht in WLC-Protokollen oder Debuggen angezeigt wird. Der Benutzer muss überprüfen, ob die vom DHCP-

Server gesendete DNS-Serverkonfiguration korrekt ist und ob sie vom Wireless-Client aus erreichbar ist. Eine einfache DNS-Suche vom nicht funktionierenden Client ist die einfachste Möglichkeit, dies zu überprüfen.

- **Standard-Gateway nicht erreichbar, wenn Sie internen DHCP-Server vor Anker verwenden:**

Wenn Sie interne DHCP-Server verwenden, muss sichergestellt werden, dass die Standard-Gateway-Konfiguration korrekt ist und das VLAN auf dem Switch-Port zugelassen ist, der mit dem Anker-WLC verbunden ist. Andernfalls erhält der Client eine IP-Adresse, aber er kann auf nichts zugreifen. Sie können die ARP-Tabelle auf dem Client auf die MAC-Adresse des Kabelmodems überprüfen. So können Sie schnell überprüfen, ob die L2-Verbindung mit dem Gateway erreichbar ist.