Fehlerbehebung bei Identity PSK auf Wireless LAN-Controllern

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie Probleme mit PSK-Verbindungen (Identity Pre-Shared Key) auf dem Cisco Wireless LAN Controller (WLC) beheben können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco WLC mit Code 8.5 und höher und Identity Services Engine (ISE)
- Zentrales Switched WLAN (FlexConnect Local Switching with Identity PSK wird derzeit nicht unterstützt)
- Identity PSK-Konfiguration auf dem WLC und der ISE. Diese finden Sie unter:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-5/b_Identity_PSK_Feature_Deployment_Guide.html

Verwendete Komponenten

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

- Cisco WLC der Serie 5508 mit Softwareversion 8.5.103.0
- Cisco ISE mit Version 2.2

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Identitäts-PSK im Überblick

Schritt 1: Der Client sendet eine Zuordnungsanfrage an den mit PSK+MAC-Authentifizierung aktivierten Service Set Identifier (SSID).

Schritt 2: Da die WLC-Kontakte durch die MAC-Authentifizierung aktiviert wurden, muss der Radius-Server die MAC-Adresse des Clients überprüfen.

Schritt 3: Der Radius-Server überprüft die Client-Details und sendet die Cisco Av-Paare, für die er PSK als Authentifizierungstyp sowie den für den Client zu verwendenden Schlüsselwert angibt.

Schritt 4: Sobald dieser empfangen wurde, sendet der WLC die Zuordnungsantwort an den Client. Dieser Schritt ist wichtig, da die Kommunikation zwischen dem WLC und dem Radius-Server verzögert wird, können Clients in einer Assoziations-Schleife stecken, in der sie eine zweite Zuordnungsanfrage senden, bevor die Antwort vom Radius-Server empfangen wird.

Schritt 5: Der WLC verwendet den vom Radius-Server gesendeten Schlüsselwert als PMK-Schlüssel. Der Access Point (AP) fährt dann mit dem Vier-Wege-Handshake fort, der überprüft, ob das auf dem Client konfigurierte Kennwort mit dem vom Radius-Server gesendeten Wert übereinstimmt.

Schritt 6: Der Client schließt dann den DHCP-Prozess ab und wechselt ebenfalls in den RUN-Status.

Problembehebungsszenarien

Diese Debug-Schritte sind erforderlich, um Identitäts-PSK-Probleme zu beheben:

Debugger auf dem WLC:

- **debug client_mac,** wobei **client _mac** die MAC-Adresse des Clienttests ist.
- **debuggen aaa detail enable**

Szenario 1. Szenario bestehen, in dem der Client erfolgreich verbunden ist

Der Client sendet eine Zuordnungsanfrage an den Access Point:

```
*apfMsConnTask_6: Sep 21 15:01:43.496: e8:50:8b:64:4f:45 Association received from mobile on
BSSID 28:6f:7f:e2:24:cf AP AP_2802-1
```

Der WLC kontaktiert dann den Radius-Server, um die MAC-Adresse des Clients zu überprüfen:

```
*aaaQueueReader: Sep 21 15:01:43.498: AuthenticationRequest: 0x2b8c8a9c
*apfMsConnTask_6: Sep 21 15:01:43.498: e8:50:8b:64:4f:45 apfProcessAssocReq (apf_80211.c:11440)
Changing state for mobile e8:50:8b:64:4f:45 on AP 28:6f:7f:e2:24:c0 from Associated to AAA
Pending
```

```
*aaaQueueReader: Sep 21 15:01:43.498:
Callback.....................................0x10762018

*aaaQueueReader: Sep 21 15:01:43.498:
protocolType.................................0x40000001
```

Der Radius-Server antwortet mit der Access-Accept-Nachricht, die auch den PSK-Methodentyp und -Schlüssel enthält, der für die Authentifizierung verwendet wird:

```
*radiusTransportThread: Sep 21 15:01:43.794: AuthorizationResponse: 0x171b5c00

*radiusTransportThread: Sep 21 15:01:43.794:
structureSize................................313

*radiusTransportThread: Sep 21 15:01:43.794:
resultCode...................................0


*radiusTransportThread: Sep 21 15:01:43.794:         Packet contains 5 AVPs:

*radiusTransportThread: Sep 21 15:01:43.794:             AVP[01] User-
Name.............................E8-50-8B-64-4F-45 (17 bytes)

*radiusTransportThread: Sep 21 15:01:43.794:             AVP[02]
State....................................ReauthSession:0a6a20770000000059c346ed (38 bytes)

*radiusTransportThread: Sep 21 15:01:43.794:             AVP[03]
Class....................................CACS:0a6a20770000000059c346ed:ISE/291984633/6 (45
bytes)

*radiusTransportThread: Sep 21 15:01:43.794:             AVP[04] Cisco / PSK-
Mode.......................ascii (5 bytes)

*radiusTransportThread: Sep 21 15:01:43.794:             AVP[05] Cisco /
PSK............................cisco123 (8 bytes)
```

Nach Erhalt dieser Nachricht sendet der WLC die Zuordnungsantwort, und es geschieht ein vierfaches Handshake:

```
*apfReceiveTask: Sep 21 15:01:43.924: e8:50:8b:64:4f:45 Sending assoc-resp with status 0
station:e8:50:8b:64:4f:45 AP:28:6f:7f:e2:24:c0-01 on apVapId 1
```

Der Vierwege-Handshake:

```
*Dot1x_NW_MsgTask_5: Sep 21 15:01:43.994: e8:50:8b:64:4f:45 Sending EAPOL-Key Message to mobile
e8:50:8b:64:4f:45
   state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_5: Sep 21 15:01:43.998: e8:50:8b:64:4f:45 Received EAPOL-key in PTK_START
state (message 2) from mobile e8:50:8b:64:4f:45
*Dot1x_NW_MsgTask_5: Sep 21 15:01:43.998: e8:50:8b:64:4f:45 Received valid MIC in EAPOL Key
Message M2!!!!!
*Dot1x_NW_MsgTask_5: Sep 21 15:01:43.999: e8:50:8b:64:4f:45 Sending EAPOL-Key Message to mobile
e8:50:8b:64:4f:45
   state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
```

```
*Dot1x_NW_MsgTask_5: Sep 21 15:01:44.003: e8:50:8b:64:4f:45 Received EAPOL-key in
PTKINITNEGOTIATING state (message 4) from mobile e8:50:8b:64:4f:45
```

Anschließend schließt der Client den DHCP-Prozess ab und wechselt in den RUN-Status (die Ausgabe wird geklickt, um die wichtigen Abschnitte anzuzeigen):

```
(WLC_1) >show client detail e8:50:8b:64:4f:45
Client MAC Address.............................. e8:50:8b:64:4f:45
Client Username ................................ E8-50-8B-64-4F-45
Hostname: ...................................... S6-edge
Device Type: ................................... Android-Samsung-Galaxy-Phone
AP MAC Address.................................. 28:6f:7f:e2:24:c0
AP Name......................................... AP_2802-1
Wireless LAN Network Name (SSID)................ Identity PSK
Wireless LAN Profile Name....................... Identity PSK
Security Policy Completed....................... Yes
Policy Manager State............................ RUN
```

Szenario 2. Client versucht, Verbindung mit falschem Kennwort herzustellen

Die erste Reihenfolge der Schritte entspricht der einer bestanden Authentifizierung.

- Der Client sendet eine Zuordnungsanfrage.
- Sobald der WLC dies erhält, initiiert er die Kommunikation mit dem Radius-Server, um die MAC-Adresse des Clients zu überprüfen.
- Wenn der Radius-Server über die Client-Details verfügt, sendet er eine access-accept mit dem Schlüsselwert und dem Authentifizierungstyp PSK.
- Der nützliche Bereich, in dem der Fehler bemerkt werden kann, ist der vierseitige Handshake.

Der Access Point sendet die Meldung 1, an die der Client mit der Meldung 2 antwortet:

```
*Dot1x_NW_MsgTask_7: Sep 21 15:12:47.661: 50:8f:4c:9d:ef:87 Received EAPOL-key in PTK_START
state (message 2) from mobile 50:8f:4c:9d:ef:87
```

Aufgrund unterschiedlicher PMK-Schlüsselwerte (Kennwort) leiten der Access Point und der Client jedoch verschiedene Schlüssel ab, was in Nachricht 2 zu einem ungültigen MIC-Empfang führt:

```
*Dot1x_NW_MsgTask_7: Sep 21 15:12:47.662: 50:8f:4c:9d:ef:87 Received EAPOL-key M2 with invalid
MIC from mobile 50:8f:4c:9d:ef:87 version 2
*osapiBsnTimer: Sep 21 15:12:48.824: 50:8f:4c:9d:ef:87 802.1x 'timeoutEvt' Timer expired for
station 50:8f:4c:9d:ef:87 and for message = M2
*Dot1x_NW_MsgTask_7: Sep 21 15:12:48.824: 50:8f:4c:9d:ef:87 Retransmit 1 of EAPOL-Key M1 (length
121) for mobile 50:8f:4c:9d:ef:87

The client then is then de-authenticated by the WLC:
*Dot1x_NW_MsgTask_7: Sep 21 15:12:50.825: 50:8f:4c:9d:ef:87 Sent Deauthenticate to mobile on
BSSID 28:6f:7f:e2:24:c0 slot 0(caller 1x_ptsm.c:655)

<noscript>
```

Eine weitere nützliche Ausgabe, die überprüft werden kann, ist die 'show client detail'. Hier sehen Sie, dass der Client im START-Status steckt:

```
*Dot1x_NW_MsgTask_7: Sep 21 15:12:47.662: 50:8f:4c:9d:ef:87 Received EAPOL-key M2 with invalid
MIC from mobile 50:8f:4c:9d:ef:87 version 2
*osapiBsnTimer: Sep 21 15:12:48.824: 50:8f:4c:9d:ef:87 802.1x 'timeoutEvt' Timer expired for
station 50:8f:4c:9d:ef:87 and for message = M2
*Dot1x_NW_MsgTask_7: Sep 21 15:12:48.824: 50:8f:4c:9d:ef:87 Retransmit 1 of EAPOL-Key M1 (length
121) for mobile 50:8f:4c:9d:ef:87
```

```
The client will then be de-authenticated by the WLC:
*Dot1x_NW_MsgTask_7: Sep 21 15:12:50.825: 50:8f:4c:9d:ef:87 Sent Deauthenticate to mobile on
BSSID 28:6f:7f:e2:24:c0 slot 0(caller 1x_ptsm.c:655)
```

Szenario 3. Radius-Server nicht erreichbar

Der WLC versucht, den Radius-Server zu kontaktieren, sobald er die Zuordnungsanfrage erhält. Falls der Radius-Server nicht erreichbar ist, versucht der WLC wiederholt, den Radius-Server zu kontaktieren (bis die Wiederholungszahl erreicht ist). Sobald der Radius-Server nach der konfigurierten Anzahl von Wiederholungen als nicht erreichbar erkannt wurde (Standardwert ist 5), sendet der WLC eine Zuordnungsantwort mit Statuscode 1, wie hier gezeigt:

```
*apfReceiveTask: Sep 21 15:28:55.777: 50:8f:4c:9d:ef:87 Sending assoc-resp with status 1
station:50:8f:4c:9d:ef:87 AP:a0:e0:af:62:f3:c0-00 on apVapId 1
*apfReceiveTask: Sep 21 15:28:55.777: 50:8f:4c:9d:ef:87 Sending Assoc Response (status:
'unspecified failure') to station on AP AP_2802-2 on BSSID a0:e0:af:62:f3:c0 ApVapId 1 Slot 0,
mobility role 0
```

Sie können auch die Anzahl der Wiederholungsanfragen und Timeout-Anfragen sehen, die in der Radius-Server-Statistik wächst, für die Sie zu **Monitor > Statistics > RADIUS Servers** navigieren können, wie im Bild gezeigt:

Szenario 4. Der vom Radius-Server gesendete Parameter für die Außerkraftsetzung

ist falsch.

Es gibt mehrere Parameter, die zusammen mit PSK und dem Schlüssel gesendet werden können, z. B. VLAN, ACL und Benutzerrolle. Wenn der vom Radius-Server gesendete ACL-Eintrag jedoch nicht konfiguriert ist, lehnt der WLC den Client ab, selbst wenn der Radius-Server die Authentifizierungsanforderung genehmigt. Dies wird im Clientdebuggen deutlich angezeigt:

```
*radiusTransportThread: Sep 22 14:39:05.499: AuthorizationResponse: 0x171b5c00

*radiusTransportThread: Sep 22 14:39:05.499:
structureSize.............................376

*radiusTransportThread: Sep 22 14:39:05.499:
resultCode................................0

*radiusTransportThread: Sep 22 14:39:05.499:
protocolUsed..............................0x00000001

*radiusTransportThread: Sep 22 14:39:05.499:         Packet contains 7 AVPs:

*radiusTransportThread: Sep 22 14:39:05.499:             AVP[01] User-
Name..............................E8-50-8B-64-4F-45 (17 bytes)

*radiusTransportThread: Sep 22 14:39:05.499:             AVP[02]
State.................................ReauthSession:0a6a20770000002659c493e9 (38 bytes)

*radiusTransportThread: Sep 22 14:39:05.499:             AVP[03]
Class.................................CACS:0a6a20770000002659c493e9:ISE/291984633/78 (46
bytes)

*radiusTransportThread: Sep 22 14:39:05.499:             AVP[04] Cisco / PSK-
Mode.....................ascii (5 bytes)

*radiusTransportThread: Sep 22 14:39:05.499:             AVP[05] Cisco /
PSK............................cisco123 (8 bytes)

*radiusTransportThread: Sep 22 14:39:05.499:             AVP[06] Unknown Cisco / Attribute
19............teacher (7 bytes)

*radiusTransportThread: Sep 22 14:39:05.499:             AVP[07] Airespace / ACL-
Name.....................testing (7 bytes)
```

Client-Debuggen:

```
*apfReceiveTask: Sep 22 14:39:05.564: e8:50:8b:64:4f:45  ACL received from RADIUS does not exist
in WLC de-authenticating the client
*apfReceiveTask: Sep 22 14:39:05.628: e8:50:8b:64:4f:45 Sending assoc-resp with status 12
station:e8:50:8b:64:4f:45 AP:28:6f:7f:e2:24:c0-01 on apVapId 1
```

Szenario 5. Client-Richtlinie auf RADIUS-Server nicht konfiguriert

Wenn der Radius-Server erreichbar ist, aber auf dem Radius-Server für den Client keine Richtlinien konfiguriert sind, kann er nur mit dem PSK verbunden werden, der global unter dem WLAN konfiguriert ist. Alle anderen Einträge sind fehlerhaft. Es gibt nichts Spezielles, das zwischen einer funktionierenden globalen PSK-Authentifizierung und einer funktionierenden Identität PSK-Authentifizierung unterschieden werden kann, außer in der Ausgabe für Debug Authentication, Authorization, and Accounting (AAA), bei der keine überschriebenen Parameter

überschrieben werden:

```
*radiusTransportThread: Sep 22 14:32:13.734: AuthorizationResponse: 0x171b5c00

*radiusTransportThread: Sep 22 14:32:13.734:
structureSize.............................269

*radiusTransportThread: Sep 22 14:32:13.734:
resultCode................................0

*radiusTransportThread: Sep 22 14:32:13.734:
protocolUsed..............................0x00000001

*radiusTransportThread: Sep 22 14:32:13.734:
proxyState................................50:8F:4C:9D:EF:87-00:00

*radiusTransportThread: Sep 22 14:32:13.734:         Packet contains 3 AVPs:

*radiusTransportThread: Sep 22 14:32:13.734:             AVP[01] User-
Name..............................50-8F-4C-9D-EF-87 (17 bytes)

*radiusTransportThread: Sep 22 14:32:13.734:             AVP[02]
State.................................ReauthSession:0a6a20770000002359c49240 (38 bytes)

*radiusTransportThread: Sep 22 14:32:13.734:             AVP[03]
Class.................................CACS:0a6a20770000002359c49240:ISE/291984633/74 (46
bytes)
```