對無線LAN控制器上的身份PSK進行故障排除

目錄

簡介

本檔案介紹如何對思科無線LAN控制器(WLC)上的身分預先共用金鑰(PSK)連線問題進行疑難排解。

必要條件

需求

思科建議您瞭解以下主題：

- 執行代碼8.5及更高版本的Cisco WLC和身分識別服務引擎(ISE)
- 集中交換WLAN（目前不支援使用身分PSK的FlexConnect本地交換）
- WLC和ISE上的身份PSK配置。可以在以下連結中找到：

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

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 5508系列WLC（執行軟體版本8.5.103.0）
- 運行2.2版的Cisco 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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

瞭解身份PSK流程

步驟1.客戶端向啟用了PSK+MAC身份驗證的服務集識別符號(SSID)傳送關聯請求。

步驟2.由於MAC身份驗證已啟用WLC聯絡人，因此radius伺服器將驗證客戶端的MAC地址。

步驟3. Radius伺服器驗證使用者端詳細資訊，並傳送其指定將PSK作為要使用的驗證型別以及要用於使用者端的金鑰值的Cisco av配對。

步驟4.收到此指令後，WLC會將關聯回應傳送到使用者端。請務必注意此步驟，因為WLC和radius伺服器之間的通訊發生延遲時，使用者端可能會停滯在關聯回圈中，他們在從radius伺服器收到回應之前傳送第二個關聯要求。

步驟5. WLC使用radius伺服器傳送的金鑰值作為PMK金鑰。存取點(AP)接著進行四次交涉，驗證使用者端上設定的密碼是否與radius伺服器傳送的值相符。

步驟6.然後客戶端完成DHCP過程並進入RUN狀態。

疑難排解案例

解決身份PSK問題需要以下調試：

WLC上的調試：

- debug client client_mac， 其中**client _mac是客戶端測試的MAC地址。**
- **debug aaa detail enable**

案例1.傳送客戶機成功連線的案例

客戶端將關聯請求傳送到AP:

```
*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
```

然後WLC聯絡radius伺服器以驗證使用者端MAC位址：

```
*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
```

Radius伺服器會使用Access-Accept訊息加以回應，該訊息也包含用於驗證的PSK方法型別和金鑰：

```
*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)
```

收到此訊息後，您可以看到WLC傳送關聯回應，並且發生四次握手：

```
*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
```

四向握手：

```
*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
```

完成此操作後，客戶端完成DHCP過程並進入RUN狀態（將剪下輸出以顯示重要部分）：

```
(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
```

案例2.使用者端嘗試使用不正確的密碼連線

初始步驟順序與通過身份驗證的步驟順序相同。

- 客戶端傳送關聯請求。
- WLC收到此訊息後，會啟動與radius伺服器的通訊以驗證使用者端MAC位址。
- 如果radius伺服器有使用者端詳細資訊，它就會傳送存取接受，其中包含金鑰值和驗證型別PSK。
- 可以看到故障的有用部分是四次握手。

AP傳送消息1，客戶端將用消息2響應消息1:

```
*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
```

但是，由於PMK金鑰值（密碼）不同，AP和客戶端會生成不同的金鑰，從而導致消息2中的MIC接收無效：

```
*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>
```

要檢查的另一個有用輸出是「show client detail」。 在此您可以看到使用者端停滯在START狀態：

```
*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)
```

案例3. Radius伺服器無法連線

WLC收到關聯請求後，會嘗試連線radius伺服器。如果radius伺服器無法連線，WLC會反複嘗試連線radius伺服器（直到達到重試次數為止）。 在設定的重試次數（預設值為5）後檢測到radius伺服器無法連線後，WLC會傳送狀態碼為1的關聯回應，如下所示：

```
*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
```

您還可以看到radius伺服器統計資訊中的重試要求數和逾時要求數，您可以導覽至**Monitor > Statistics > RADIUS Servers**，如下圖所示：

案例4. Radius伺服器傳送的覆寫引數不正確

有多個引數可以與PSK和金鑰一起推送，例如VLAN、ACL和使用者角色。但是，如果沒有設定radius伺服器傳送的ACL專案，則WLC會拒絕使用者端，即使radius伺服器批准驗證要求也是如此。這可以從客戶端調試中清楚地看到：

```
*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)
```

客戶端調試：

```
*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
```

案例5. Radius伺服器上未設定使用者端原則

當RADIUS伺服器可連線但使用者端的RADIUS伺服器沒有設定原則時，只有使用WLAN下全域性設定的PSK時，才能連線。任何其他條目都將失敗。除了在調試身份驗證、授權和記帳(AAA)輸出中沒有任何特定內容來區分工作的全域性PSK身份驗證和工作身份PSK身份驗證，該輸出沒有任何被推送的覆蓋引數：

```
*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)
```