Risoluzione dei problemi relativi alla chiave PSK di identità sui controller LAN wireless

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Informazioni sul flusso di Identity PSK](#)
[Risoluzione dei problemi](#)
[Scenario 1. Passare lo scenario in cui il client si connette correttamente](#)
[Scenario 2. Tentativi di connessione del client con password non corretta](#)
[Scenario 3. Server Radius non raggiungibile](#)
[Scenario 4. Parametro di sostituzione non corretto inviato dal server Radius](#)
[Scenario 5. Criterio client non configurato nel server Radius](#)

Introduzione

In questo documento viene descritto come risolvere i problemi di connessione della chiave già condivisa dell'identità (PSK) sul controller WLC di Cisco.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco WLC con codice 8.5 e versioni successive e Identity Services Engine (ISE)
- WLAN con commutazione centrale (la commutazione locale FlexConnect con chiave già condivisa Identity non è attualmente supportata)
- Configurazione Identity PSK sul WLC e ISE. Disponibile al seguente link:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 5508 WLC con software versione 8.5.103.0
- Cisco ISE con versione 2.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Informazioni sul flusso di Identity PSK

Passaggio 1. Il client invia una richiesta di associazione all'SSID (Service Set Identifier) abilitato con l'autenticazione PSK+MAC.

Passaggio 2. Poiché l'autenticazione MAC ha abilitato i contatti WLC, il server radius deve verificare l'indirizzo MAC del client.

Passaggio 3. Il server Radius verifica i dettagli del client e invia le coppie av Cisco per le quali specifica PSK come tipo di autenticazione da utilizzare e il valore della chiave da utilizzare per il client.

Passaggio 4. Dopo aver ricevuto questa risposta, il WLC invia la risposta dell'associazione al client. È importante essere a conoscenza di questo passaggio, come se ci fosse un ritardo nella comunicazione tra il WLC e il server radius, i client possono rimanere bloccati in un loop di associazione, dove inviano una seconda richiesta di associazione prima che la risposta venga ricevuta dal server radius.

Passaggio 5. Il WLC utilizza il valore della chiave inviato dal server radius come chiave PMK. Il punto di accesso procede quindi con l'handshake a quattro vie che verifica che la password configurata nel client corrisponda al valore inviato dal server RADIUS.

Passaggio 6. Il client completa quindi il processo DHCP e passa anche allo stato RUN.

Risoluzione dei problemi

Questi debug sono necessari per risolvere i problemi relativi a Identity PSK:

Debug sul WLC:

- **debug client_mac,** dove **_mac client** è l'indirizzo MAC del test del client.
- **abilitazione dettagli debug aaa**

Scenario 1. Passare lo scenario in cui il client si connette correttamente

Il client invia la richiesta di associazione all'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
```

Il WLC contatta quindi il server radius per verificare l'indirizzo MAC del client:

```
*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
```

Il server radius risponde con il messaggio Access-Accept che contiene anche il tipo di metodo PSK e la chiave utilizzata per l'autenticazione:

```
*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)
```

Una volta ricevuta la risposta, il WLC la invia all'associazione e si verifica un handshake a quattro vie:

```
*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
```

La stretta di mano a quattro vie:

```
*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
```

Al termine, il client completa il processo DHCP e passa allo stato RUN (l'output viene troncato per visualizzare le sezioni importanti):

```
(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
```

Scenario 2. Tentativi di connessione del client con password non corretta

La sequenza iniziale dei passaggi rimane la stessa di un'autenticazione passata.

- Il client invia una richiesta di associazione.
- Una volta ricevuto questo messaggio, il WLC avvia la comunicazione con il server radius per verificare l'indirizzo MAC del client.
- Se il server radius dispone dei dettagli del client, invia un messaggio di accettazione dell'accesso con il valore della chiave e il tipo di autenticazione PSK.
- La sezione utile in cui è possibile notare l'errore è la stretta di mano a quattro vie.

L'access point invia il messaggio 1, al quale il client risponde con il messaggio 2:

```
*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
```

Tuttavia, a causa dei diversi valori della chiave PMK (password), l'access point e il client derivano chiavi diverse, il che determina una conferma MIC non valida nel messaggio 2:

```
*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>
```

Un altro output utile da controllare è il comando "show client detail". Qui è possibile vedere il client è bloccato in stato START:

```
*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)
```

Scenario 3. Server Radius non raggiungibile

Il WLC tenta di contattare il server radius dopo aver ricevuto la richiesta di associazione. Se il server radius non è raggiungibile, il WLC tenta ripetutamente di contattare il server radius (fino a raggiungere il numero di tentativi). Quando il server radius viene rilevato come non raggiungibile dopo il numero di tentativi configurato (il valore predefinito è 5), il WLC invia una risposta di associazione con il codice di stato 1, come mostrato di seguito:

```
*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
```

Èinoltre possibile visualizzare il numero di richieste di nuovi tentativi e di timeout che aumenta nelle statistiche del server RADIUS, per le quali è possibile passare a **Monitoraggio > Statistiche > Server RADIUS** come mostrato nell'immagine:

Scenario 4. Parametro di sostituzione non corretto inviato dal server Radius

Èpossibile eseguire il push di diversi parametri insieme alla chiave PSK e alla chiave, ad esempio VLAN, ACL e ruolo utente. Tuttavia, se la voce ACL inviata dal server radius non è configurata, il WLC rifiuta il client, anche se il server radius approva la richiesta di autenticazione. Questa condizione può essere rilevata chiaramente nei debug del client:

```
*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)
```

Debug del client:

```
*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
```

Scenario 5. Criterio client non configurato nel server Radius

Quando il server radius è raggiungibile ma non è configurato alcun criterio sul server radius per il client, può essere connesso solo se utilizza la chiave PSK, configurata globalmente nella rete WLAN. Qualsiasi altra voce fallirebbe. Non vi sono elementi specifici per distinguere tra un'autenticazione PSK globale funzionante e un'autenticazione PSK identità funzionante, ad eccezione dell'output di debug Authentication, Authorization, and Accounting (AAA) che non avrà parametri di sostituzione sottoposti a push:

```
*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)
```