Dépannage de la clé PSK d'identité sur les contrôleurs de réseau local sans fil

Contenu

Introduction

Ce document décrit comment résoudre les problèmes de connexion à la clé prépartagée d'identité (PSK) sur le contrôleur de réseau local sans fil (WLC) Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco WLC qui exécute le code 8.5 et les versions ultérieures et Identity Services Engine (ISE)
- WLAN à commutation centralisée (la commutation locale FlexConnect avec Identity PSK n'est pas prise en charge actuellement)
- Configuration PSK d'identité sur le WLC et ISE. Vous pouvez le trouver sur ce lien : https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-5/b_Identity_PSK_Feature_Deployment_Guide.html

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC de la gamme Cisco 5508 qui exécute le logiciel version 8.5.103.0
- Cisco ISE qui exécute la version 2.2

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Comprendre le flux d'identités PSK

Étape 1. Le client envoie une demande d'association au SSID (Service Set Identifier) activé avec l'authentification PSK+MAC.

Étape 2. Puisque l'authentification MAC a activé les contacts WLC, le serveur radius doit vérifier l'adresse MAC du client.

Étape 3. Le serveur Radius vérifie les détails du client et envoie les paires av Cisco pour lesquelles il spécifie PSK comme type d'authentification à utiliser ainsi que la valeur de clé à utiliser pour le client.

Étape 4. Une fois reçu, le WLC envoie la réponse d'association au client. Il est important d'être conscient de cette étape, comme s'il y a un retard dans la communication entre le WLC et le serveur radius, les clients peuvent être bloqués dans une boucle d'association, où ils envoient une deuxième demande d'association avant que la réponse ne soit reçue du serveur radius.

Étape 5. Le WLC utilise la valeur de clé envoyée par le serveur radius comme clé PMK. Le point d'accès (AP) procède ensuite avec la connexion en quatre étapes qui vérifie que le mot de passe configuré sur le client correspond à la valeur envoyée par le serveur radius.

Étape 6. Le client termine ensuite le processus DHCP et passe également à l'état EXÉCUTION.

Dépannage des scénarios

Ces débogages sont nécessaires pour résoudre les problèmes liés à l'identité PSK :

Débogues sur le WLC :

- **debug client client_mac,** où **client _mac** est l'adresse MAC du test du client.
- **debug aaa detail enable**

Scénario 1. Scénario de réussite de la connexion du client

Le client envoie la demande d'association au point d'accès :

```
*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
```

Le WLC contacte ensuite le serveur radius pour vérifier l'adresse MAC du 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
```

Le serveur radius répond avec le message Access-Accept qui contient également le type de méthode et la clé PSK utilisés pour l'authentification :

```
*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)
```

Une fois reçu, vous pouvez voir que le WLC envoie une réponse d'association et qu'une connexion en quatre étapes se produit :

```
*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 connexion en quatre étapes :

```
*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
```

Une fois que cela est fait, le client termine le processus DHCP et passe à l'état RUN (le résultat est coupé pour afficher les sections importantes) :

```
(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
```

Scénario 2. Le client tente de se connecter avec un mot de passe incorrect

La séquence initiale des étapes reste identique à celle d'une authentification passée.

- Le client envoie une demande d'association.
- Une fois que le WLC a reçu ce message, il initie la communication avec le serveur radius pour vérifier l'adresse MAC du client.
- Si le serveur radius a les détails du client, il envoie un access-accept avec la valeur de clé et le type d'authentification PSK.
- La section utile où la défaillance peut être détectée se trouve dans la connexion en quatre étapes.

Le point d’accès envoie le message 1, auquel le client répond par le message 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
```

Cependant, en raison de différentes valeurs de clé PMK (mot de passe), le point d'accès et le client dérivent des clés différentes, ce qui entraîne un reçu MIC non valide dans le message 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>
```

Une autre sortie utile à vérifier est 'show client detail'. Vous pouvez voir ici que le client est coincé dans l'état 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)
```

Scénario 3. Serveur Radius inaccessible

Le WLC tente de contacter le serveur radius une fois qu'il a reçu la demande d'association. Si le serveur radius est inaccessible, le WLC tente à plusieurs reprises de contacter le serveur radius (jusqu'à ce que le nombre de nouvelles tentatives soit atteint). Une fois que le serveur radius est détecté comme inaccessible après le nombre configuré de tentatives (la valeur par défaut est 5), le WLC envoie une réponse d'association avec le code d'état 1 comme indiqué ici :

```
*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
```

Vous pouvez également voir le nombre de demandes de nouvelle tentative et de demandes d'expiration qui augmente dans les statistiques du serveur radius, pour lesquelles vous pouvez naviguer jusqu'à **Monitor > Statistics > RADIUS Servers** comme indiqué dans l'image :

Scénario 4 . Paramètre de remplacement incorrect envoyé par le serveur Radius

Il existe plusieurs paramètres qui peuvent être appliqués avec PSK et la clé, tels que VLAN, ACL et User Role. Cependant, si l'entrée ACL envoyée par le serveur radius n'est pas configurée, le WLC rejette le client, même si le serveur radius approuve la demande d'authentification. Ceci peut être clairement visible dans les débogages clients :

```
*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)
```

Débogues 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
```

Scénario 5. Stratégie client non configurée sur le serveur Radius

Lorsque le serveur radius est accessible mais qu'aucune stratégie n'est configurée sur le serveur radius du client, il ne peut être connecté que s'il utilise le PSK, configuré globalement sous le WLAN. Toute autre entrée échouerait. Il n'y a rien de spécifique à la différenciation entre une authentification PSK globale fonctionnelle et une authentification PSK d'identité fonctionnelle, sauf dans la sortie AAA (Debug Authentication, Authorization, and Accounting) qui ne contiendra aucun paramètre de remplacement qui sera poussé :

```
*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)
```