Pesquise defeitos a identidade PSK em controladores do Wireless LAN

Índice

Introdução

Este original descreve como pesquisar defeitos questões de conexão da chave pré-compartilhada da identidade (PSK) no controlador de LAN do Cisco Wireless (WLC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco WLC que executa o código 8.5 e mais atrasado e o Identity Services Engine (ISE)
- WLAN centralmente comutado (o switching local de FlexConnect com identidade PSK não é apoiado atualmente)
- Configuração da identidade PSK no WLC e no ISE. Isto pode ser encontrado neste link:

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

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 5508 Series WLC que executa o Software Release 8.5.103.0
- Cisco ISE que executa a versão 2.2

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto

potencial de qualquer comando.

Compreenda o fluxo da identidade PSK

Etapa 1. O cliente envia um pedido da associação ao Service Set Identifier (SSID) permitido com autenticação PSK+MAC.

Etapa 2. Desde que a autenticação de MAC permitiu os contatos WLC, o servidor Radius é verificar o MAC address do cliente.

Etapa 3. O servidor Radius verifica os detalhes do cliente e envia os pares Cisco AV para que especifica o PSK enquanto o tipo do autenticação a ser usados assim como o valor chave a ser usado para o cliente.

Etapa 4. Uma vez que isto é recebido o WLC envia a resposta da associação ao cliente. É importante estar ciente desta etapa, como se há um atraso na comunicação entre o WLC e o servidor Radius, clientes pode obter colado em um laço da associação, onde enviem um segundo pedido da associação antes que a resposta esteja recebida do servidor Radius.

Etapa 5. O WLC usa o valor chave enviado pelo servidor Radius como o chave mestre. O Access Point (AP) continua então com o aperto de mão de quatro vias que verifica que a senha configurada no cliente combina o valor enviado pelo servidor Radius.

Etapa 6. O cliente então termina o processo DHCP e move-se no estado de CORRIDA também.

Pesquise defeitos encenações

Estes debugam são exigidos para pesquisar defeitos edições da identidade PSK:

Debuga no WLC:

- **debugar o client_mac do cliente,** onde o **_mac do cliente** é o MAC address do teste do cliente.
- **debugar o detalhe aaa permitem**

Encenação da passagem da encenação 1. onde o cliente conecta com sucesso

O cliente envia o pedido da associação ao 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
```

O WLC contacta então o servidor Radius para verificar o endereço MAC de cliente:

```
*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
```

O servidor Radius responde com a mensagem da aceitação de acesso que igualmente contém o tipo e a chave do método PSK que é usada para a autenticação:

```
*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)
```

Uma vez que isto é recebido você pode ver que o WLC envia a resposta da associação e um aperto de mão de quatro vias acontece:

```
*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
```

O aperto de mão de quatro vias:

```
*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
```

Uma vez que isto é feito, o cliente termina o processo DHCP e entra no estado de CORRIDA (a

saída é grampeada para mostrar as seções 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
```

Tentativas do cliente da encenação 2. a conectar com a senha incorreta

A sequência inicial das etapas fica o mesmos que aquele de uma autenticação passada.

- O cliente envia um pedido da associação.
- Uma vez que o WLC recebe este, inicia uma comunicação com o servidor Radius para verificar o endereço MAC de cliente.
- Se o servidor Radius tem o cliente detalha-o envia uma aceitação de acesso com o valor chave e o tipo do autenticação que é PSK.
- A seção útil onde a falha pode ser observada está no aperto de mão de quatro vias.

O AP envia a mensagem 1, a que o cliente responde com mensagem 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
```

Contudo, devido aos valores de chave mestre diferentes (senha) o AP e o cliente derivam chaves diferentes que conduz a um recibo inválido MIC na mensagem 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>
```

Uma outra saída útil a verificar é da “o detalhe do cliente mostra”. Aqui você pode ver que o cliente está colado no estado do COMEÇO:

```
*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
```

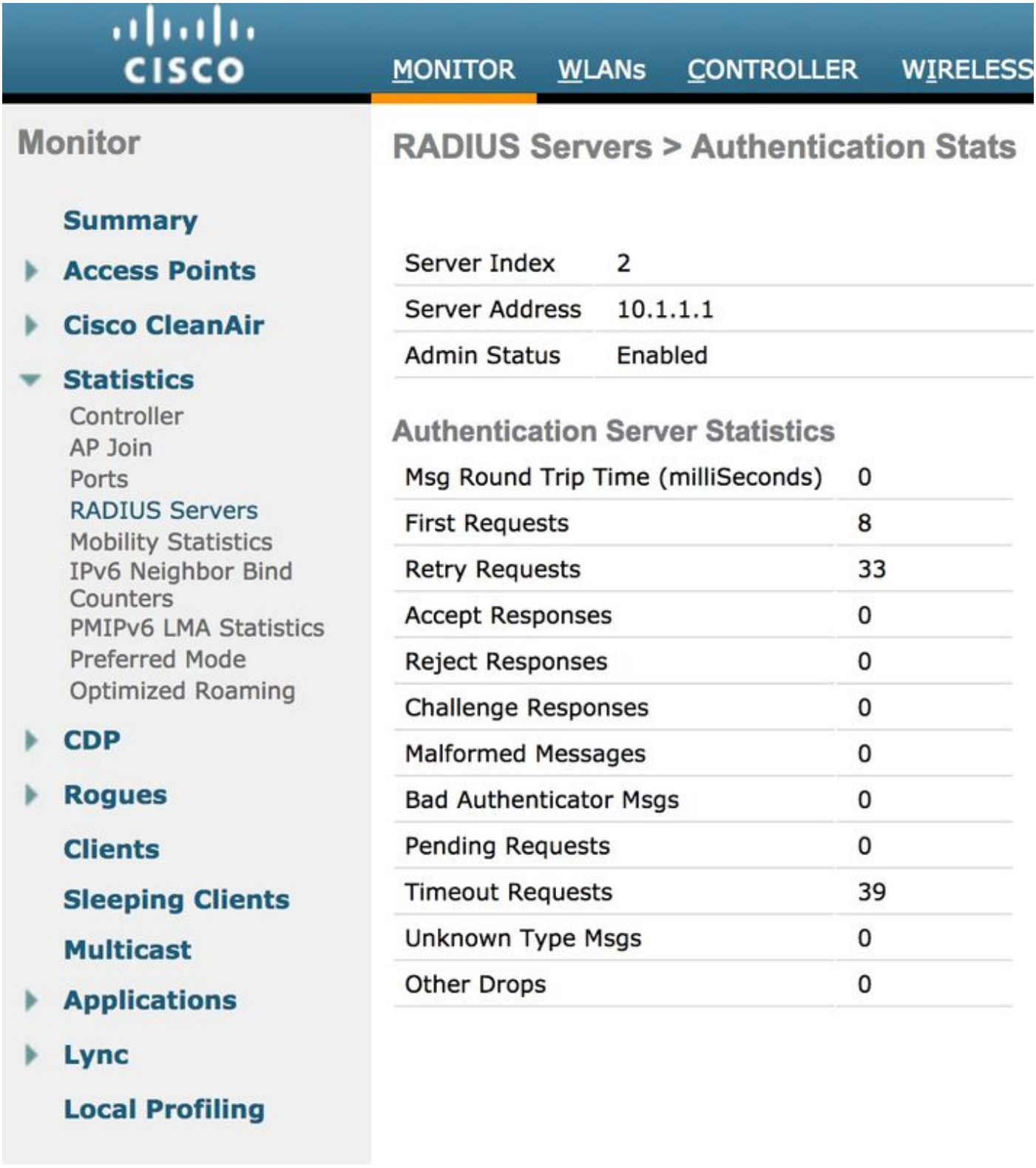
```
BSSID 28:6f:7f:e2:24:c0 slot 0(caller 1x_ptsm.c:655)
```

Servidor Radius da encenação 3. inacessível

As tentativas WLC para contactar o servidor Radius uma vez que recebe o pedido da associação. Caso que o servidor Radius é inacessível, o WLC tenta repetidamente contactar o servidor Radius (até que o contagem de novas tentativas esteja alcançado). Uma vez que o servidor Radius é detectado para ser inacessível depois que o número configurado de novas tentativas (o valor padrão é 5) o WLC envia uma resposta da associação com código de status 1 como mostrado aqui:

```
*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
```

Você pode igualmente ver que o número de pedidos e de intervalo da nova tentativa pede qual cresce nas estatísticas do servidor Radius, para que você pode navegar **para monitorar > estatísticas > servidores Radius** segundo as indicações da imagem:



Parâmetro incorreto da ultrapassagem da encenação 4. enviado pelo servidor Radius

Há diversos parâmetros que podem ser empurrados junto com o PSK e a chave, tal como o VLAN, o ACL e o papel de usuário. Contudo, se a entrada ACL enviada pelo servidor Radius não é configurada então o WLC rejeita o cliente, mesmo se o servidor Radius aprova o pedido de autenticação. Isto pode claramente ser visto no cliente debuga:

```
*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)
```

O cliente debuga:

```
*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
```

Política de cliente da encenação 5. não configurada no servidor Radius

Quando o servidor Radius é alcançável mas não há nenhuma política configurada no servidor Radius para o cliente, pode obter conectado somente se usa o PSK, configurado globalmente sob o WLAN. Todas as outras entradas falhariam. Não há nada específico para diferenciar-se entre uma autenticação global de trabalho PSK e uma autenticação de trabalho da identidade PSK exceto no debug authentication, a autorização, e explicar (AAA) output que não terá nenhuns parâmetros da ultrapassagem que é empurrado:

```
*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)
```