Comprensión y solución de problemas de RADIUS CoA y mensajes de desconexión

Contenido

Introducción
Definición de mensajes CoA RADIUS
RADIUS DM
Atributos para la identificación de sesiones
Configuración de RADIUS DM
Configuración de muestra:
Ejemplos de situaciones de fallos
No se han recibido mensajes de DM en el lado de ASR 5000
El puerto UDP 3379 tiene un socket listo sin mensajes de DM
Solicitud de contabilidad
Solicitud de desconexión
Todos los atributos coinciden, pero ASR 5000 envía DM NAK con el mensaje de error: 401 - Atributo no admitido
El sistema ha configurado "no-nas-identification-check" en la línea "radius change-authorized-nas-ip". Aún se devuelve el error "NAS-Identification-Mismatch"

Introducción

Este documento describe los mensajes de desconexión RADIUS (DM).

Definición de mensajes CoA RADIUS

Se utiliza un mensaje de cambio de autorización (CoA) para cambiar los atributos y los filtros de datos asociados a una sesión de usuario. El sistema admite mensajes CoA del servidor de autenticación, autorización y contabilidad (AAA) para cambiar los filtros de datos asociados a una sesión de suscriptor.

> **Nota**: los filtros de los atributos de ID de filtro (si están presentes en la solicitud) deben configurarse en ASR 5000 para que se apliquen al tráfico de usuarios. Esta es la forma de Listas de control de acceso (ACL) y se configura en ASR 5000 con los comandos **ip access-list**.

El mensaje de solicitud de CoA debe contener atributos para identificar la sesión de usuario; los atributos y los filtros de datos deben aplicarse a la sesión de usuario. El atributo filter-id (identificador de atributo 11) contiene los nombres de los filtros. Si ASR 5000 ejecuta

correctamente la solicitud de CoA, se devuelve un ACK de CoA al servidor RADIUS y los nuevos atributos y filtros de datos se aplican a la sesión de usuario. De lo contrario, se envía una CoA NAK con la razón apropiada como un atributo de código de error sin realizar ningún cambio en la sesión de usuario.

RADIUS DM

El mensaje DM se utiliza para desconectar las sesiones de usuario en ASR 5000 de un servidor RADIUS. El mensaje de solicitud de DM debe contener los atributos necesarios para identificar la sesión de usuario. Si el sistema desconecta correctamente la sesión de usuario, DM ACK se devuelve al servidor RADIUS. De lo contrario, DM-NAK se envía con las razones de error adecuadas.

Como se mencionó anteriormente, es posible que el NAS no pueda aceptar los mensajes de solicitud de desconexión o solicitud CoA por alguna razón. El atributo de causa de error proporciona más detalles sobre la causa del problema. Puede incluirse en los mensajes Disconnect-ACK, Disconnect-NAK y CoA-NAK.

El campo Valor es de cuatro octetos, que contiene un entero que especifica la causa del error.

- Se reservan los valores **0-199** y **300-399**.
- Los valores **200-299** representan la finalización exitosa, de modo que estos valores sólo se pueden enviar dentro de un mensaje Disconnect-ACK o CoA-ACK y NO SE DEBEN enviar dentro de un Disconnect-NAK o CoA-NAK.
- Los valores **400-499** representan errores irrecuperables cometidos por el servidor RADIUS, de modo que PUEDEN enviarse dentro de los mensajes CoA-NAK o Disconnect-NAK y NO DEBEN enviarse dentro de los mensajes CoA-ACK o Disconnect-ACK.
- Los valores **500-599** representan errores fatales que ocurren en un proxy NAS o RADIUS, de modo que PUEDEN enviarse dentro de los mensajes CoA-NAK y Disconnect-NAK, y NO DEBEN enviarse dentro de los mensajes CoA-ACK o Disconnect-ACK. Los valores de causa de error DEBEN ser registrados por el servidor RADIUS.

Los valores de código de error (expresados en decimales) incluyen:

```
 #     Value
---  -----
201   Residual Session Context Removed>
202   Invalid EAP Packet (Ignored)
401   Unsupported Attribute
402   Missing Attribute
403   NAS Identification Mismatch
404   Invalid Request
405   Unsupported Service
406   Unsupported Extension
501   Administratively Prohibited
502   Request Not Routable (Proxy)
503   Session Context Not Found
504   Session Context Not Removable
505   Other Proxy Processing Error
506   Resources Unavailable
507   Request Initiated
```

Atributos para la identificación de sesiones

Para la identificación de ASR 5000, se puede utilizar uno de estos métodos:

- NAS-IP-Address (Dirección IP del NAS): la dirección IP del NAS, si está presente en la solicitud COA/DM, debe coincidir con la dirección IP del NAS ASR 5000.
- NAS-Identifier: Si este atributo está presente, su valor debe coincidir con el nas-identifier generado para la sesión de usuario.
  Se trata de un atributo obligatorio para la identificación de sesiones, si ASR 5000 se configura con el identificador NAS.

Para la identificación de la sesión de usuario, se utiliza uno de estos métodos:

- Acct-Session-ID: Si este atributo está presente, su valor debe coincidir con el acct-session-id para la sesión de usuario.
- Framed-IP-Address: si este atributo está presente, sus valores deben coincidir con la dirección IP de la sesión.
- Nombre de usuario: Si este atributo está presente, sus valores deben coincidir con el nombre de usuario de la sesión.
- Calling-Station-ID (ID de la estación de llamada): se trata de la identidad internacional del suscriptor móvil (IMSI) del usuario.

Configuración de RADIUS DM

La configuración de un RADIUS DM es bastante fácil. Todas las líneas deben configurarse en el contexto de destino (el que tiene la configuración RADIUS).

radius change-authorized-nas-ip *ip_address* **clave [cifrada]** *valor* **[puerto** *puerto* **]**
[eventtimestamp-window *ventana* **] [no-nas-identification-check]**
[no-reverse-path-forward-check][mpls-label input *in_label_value* **| resultado** *out_label_value1*
[*out_label_value2* **]**

> **Nota**: "radius change-authorized-nas-ip" debe ser la dirección de interfaz AAA de su contexto local. Este comando CLI es a veces fuente de confusión.

Configuración de muestra:

```
radius change-authorize-nas-ip 192.168.88.40 encrypted key <key value>
no-reverse-path-forward-check
no-nas-identification-check
```

Ejemplos de situaciones de fallos

No se han recibido mensajes de DM en el lado de ASR 5000

Es posible que el socket no esté listo para el puerto UDP 3799. (De acuerdo con RFC 3756, el paquete de solicitud de desconexión de RADIUS se envía al puerto UDP 3799).

Este comportamiento se puede simplificar. El proceso que maneja todas las solicitudes CoA es la instancia aamgr 385, que es la de la tarjeta SMC/MIO activa. Este comando CLI debe ejecutarse en el contexto de destino.

```
#cli test-commands password <xx> #show radius info radius group all instance 385
```

Este resultado es similar a:

```
# show radius info radius group all instance 385 AAAMGR instance 385:
cb-list-en: 3 AAA Group: <>
---------------------------------------------
socket number: 19
socket state: ready
local ip address: 10.176.81.215
local udp port: 50954
flow id: 0
use med interface: no
VRF context ID: 66
```

En este ejemplo, no hay ningún puerto 3799 y esta es la razón del comportamiento informado. Si ve lo mismo en su caso, la solución es quitar y volver a agregar la configuración de CoA para recrear el socket de escucha. Además, puede intentar eliminar la instancia 385 de aamgr si la primera solución no le ayuda.

Después de las acciones descritas, debería ver este resultado:

```
# show radius info radius group all instance 385 AAAMGR instance 385:
cb-list-en: 3 AAA Group: <>
---------------------------------------------->
socket number: 19>
socket state: ready
local ip address: 10.176.81.215
local udp port: 50954
flow id: 0
use med interface: no
VRF context ID: 66
socket number: 21   <---------------------
socket state: ready
local ip address: 10.176.81.215
local udp port: 3799 <--------------------
flow id: 0
use med interface: no
```

y el socket debe ser visible desde el shell de depuración en el contexto/VR apropiado:

```
bash-2.05b# netstat -lun | grep 3799
udp 0 0 10.176.81.215:3799 0.0.0.0:*
```

El puerto UDP 3379 tiene un socket listo sin mensajes de DM

El puerto UDP 3379 tiene un socket listo, sin embargo aún no ve los mensajes de DM. Esto es

probablemente causado por una configuración incorrecta de **radius change-authorized-nas-ip**. Los valores de atributo que vinieron en el mensaje de solicitud de DM no coinciden con los que fueron enviados en una solicitud de contabilidad hacia RADIUS.

Solicitud de contabilidad

```
Thursday August 06 2015
<<<<OUTBOUND
Code: 4 (Accounting-Request)
     Attribute Type: 44 (Acct-Session-Id)
               Length: 18
               Value: 42 43 37 31 44 46 32 36 BC71DF26
                      30 36 30 33 41 32 42 46 0603A2BF
     Attribute Type: 31 (Calling-Station-Id)
               Length: 14
               Value: 39 39 38 39 33 31 37 32 99893172
                      30 39 31 31             0911
     Attribute Type: 4 (NAS-IP-Address)
               Length: 6
               Value: C0 A8 58 E1             ..X.
                      (192.168.88.225)
     Attribute Type: 8 (Framed-IP-Address)
               Length: 6
               Value: 0A 55 12 21             .U.!
                      (10.85.18.33)
```

Solicitud de desconexión

```
Radius Protocol
   Code: Disconnect-Request (40)
   Packet identifier: 0x2 (2)
   Length: 71
   Authenticator: 4930a228f13da294550239f5187b08b9

   Attribute Value Pairs
       AVP: l=6 t=NAS-IP-Address(4): 192.168.88.225
           NAS-IP-Address: 192.168.88.225 (192.168.88.225)

       AVP: l=6 t=Framed-IP-Address(8): 10.85.18.33
           Framed-IP-Address: 10.85.18.33 (10.85.18.33)

       AVP: l=14 t=Calling-Station-Id(31): 998931720911
           Calling-Station-Id: 998931720911

       AVP: l=18 t=Acct-Session-Id(44): BC71DF260603A2BF
           Acct-Session-Id: BC71DF260603A200
```

En este ejemplo, el valor de **Acct-Session-Id** que llega a ASR 5000 es diferente del que se envía hacia RADIUS y esta es la razón del problema. Este problema puede solucionarse con cambios adecuados en el lado RADIUS.

La ID de sesión de cuenta para la sesión activa se puede verificar con el comando **show subscribers ggsn-only aaa-configuration active imsi <>**.

```
[local]# show subscribers ggsn-only aaa-configuration active imsi 434051801170727
```

```
Username: 998931720911@mihc1             Status: Online/Active
 Access Type: ggsn-pdp-type-ipv4        Network Type: IP
 Access Tech: WCDMA UTRAN               Access Network Peer ID: n/a
 callid: 057638b8                       imsi: 434051801170727
 3GPP2 Carrier ID: n/a
 3GPP2 ESN: n/a
 RADIUS Auth Server: 192.168.88.40  RADIUS Acct Server: n/a
 NAS IP Address: 192.168.88.225
 Acct-session-id: BC71DF260603A2BF
```

Todos los atributos coinciden, pero ASR 5000 envía DM NAK con el mensaje de error: 401 - Atributo no admitido

En este momento se sabe que este tipo de mensaje de error significa que el problema proviene del servidor RADIUS. Sin embargo, todavía no está claro qué es lo que está mal. Aquí, la limitación de ASR 5000 no admite Called-station-Id en Radius DM. Por lo tanto, si se ve allí, responde con el error resaltado.

```
INBOUND>>>>>
RADIUS COA Rx PDU, from 192.168.1.254:38073 to 192.168.1.2:1800
Code: 40 (Disconnect-Request)
Id: 106
Length: 61
Authenticator: 8D F1 50 2E DD 79 49 39 79 A0 B5 FC 59 3E C4 51
    Attribute Type: 32 (NAS-Identifier)
              Length: 9
              Value: 73 74 61 72 65 6E 74   starent
    Attribute Type: 1 (User-Name)
              Length: 10
              Value: 74 65 73 74 75 73 65 72 testuser
    Attribute Type: 30 (Called-Station-ID)
              Length: 9
              Value: 65 63 73 2D 61 70 6E   ecs-apn
    Attribute Type: 31 (Calling-Station-Id)
              Length: 13
              Value: 36 34 32 31 31 32 33 34 64211234
                     35 36 37               567

<<<<OUTBOUND 06:57:42:683 Eventid:70902(6)
RADIUS COA Tx PDU, from 192.168.1.2:1800 to 192.168.1.254:38073
Code: 42 (Disconnect-Nak)
Id: 106
Length: 26
Authenticator: 34 2E DE B4 77 22 4A FE A5 16 93 91 0D B2 E6 3B
    Attribute Type: 101 (Error-Cause)
              Length: 6
              Value: 00 00 01 91             ....
                      (Unsupported-Attribute)
```

El sistema ha configurado "no-nas-identification-check" en la línea "radius change-authorized-nas-ip". Aún se devuelve el error "NAS-Identification-Mismatch"

Esto sucede en esta configuración:

```
radius change-authorize-nas-ip 192.168.1.2 encrypted key
+A27wvxlgy06ia30pcqswmdajxd11ckg4ns88i6l92dghsqw7v77f1 port 1800
```

```
event-timestamp-window 0 no-reverse-path-forward-check no-nas-identification-check
   aaa group default
   radius attribute nas-ip-address address 192.168.1.2
   radius server 192.168.1.128 encrypted key
+A3ec01d8zs92ed1gz2mytddjjrf11af3u0watpyr3gd0rs8mthlzc port 1812
   radius accounting server 192.168.1.128 encrypted key
+A24x0pj4mjgnqh0sclbnen1lm6f1d6drn2nw3yf31tmfldk9fr38e         port 1813
#exit
```

Para un contexto PDP activo, la solicitud de desconexión es NAKed:

```
INBOUND>>>>>  04:27:13:898 Eventid:70901(6)
RADIUS COA Rx PDU, from 192.168.1.254:42082 to 192.168.1.2:1800 (52) PDU-dict=starent-vsa1
 Code: 40 (Disconnect-Request)
 Id: 115
 Length: 52
 Authenticator: BF 95 05 0B 87 B4 42 59 5F C6 CC 78 D7 17 77 7F
     Attribute Type: 32 (NAS-Identifier)
               Length: 9
               Value: 73 74 61 72 65 6E 74    starent
     Attribute Type: 1 (User-Name)
               Length: 10
               Value: 74 65 73 74 75 73 65 72 testuser
     Attribute Type: 31 (Calling-Station-Id)
                           Value: 36 34 32 31 31 32 33 34 64211234;     Length: 13

                      35 36 37                567

Monday October 19 2015
<<<<OUTBOUND  04:27:13:898 Eventid:70902(6)
RADIUS COA Tx PDU, from 192.168.1.2:1800 to 192.168.1.254:42082 (26) PDU-dict=starent-vsa1
 Code: 42 (Disconnect-Nak)
 Id: 115
 Length: 26
 Authenticator: 75 D1 04 3E 31 19 9C 92 B2 2E 5D 5F 98 B9 34 99
     Attribute Type: 101 (Error-Cause)
               Length: 6
               Value: 00 00 01 93             ....
                      (NAS-Identification-Mismatch)
```

Sin embargo, cuando esta línea se incluye en el grupo AAA predeterminado:

```
    radius attribute nas-identifier starent
```

empieza a funcionar:

```
Monday October 19 2015
INBOUND>>>>>  05:19:01:798 Eventid:70901(6)
RADIUS COA Rx PDU, from 192.168.1.254:55426 to 192.168.1.2:1800 (52) PDU-dict=starent-vsa1
 Code: 40 (Disconnect-Request)
 Id: 171
 Length: 52
 Authenticator: 3A 67 43 25 DC 18 5C E3 23 08 04 C0 9C 31 68 68
     NAS-Identifier = starent
     User-Name = testuser
     Calling-Station-Id = 64211234567


Monday October 19 2015
<<<<OUTBOUND  05:19:01:799 Eventid:70902(6)
RADIUS COA Tx PDU, from 192.168.1.2:1800 to 192.168.1.254:55426 (26) PDU-dict=starent-vsa1
```

```
 Code: 41 (Disconnect-Ack)
 Id: 171
 Length: 26
 Authenticator: 45 07 79 C5 E0 92 53 28 8F AD A3 E3 C4 B4 52 10
     Acct-Termination-Cause = Admin_Reset
```

O también funcionará sin la configuración del identificador nas en el grupo AAA, pero con el AVP del identificador NAS eliminado de la solicitud de desconexión:

```
INBOUND>>>>>  05:14:41:374 Eventid:70901(6)
RADIUS COA Rx PDU, from 192.168.1.254:54757 to 192.168.1.2:1800 (43) PDU-dict=starent-vsa1
 Code: 40 (Disconnect-Request)
 Id: 78
 Length: 43
 Authenticator: 84 5D FE 5E 90 0D C8 16 84 7A 11 67 FF 82 40 DB
     User-Name = testuser
     Calling-Station-Id = 64211234567

Monday October 19 2015
<<<<OUTBOUND  05:14:41:375 Eventid:70902(6
RADIUS COA Tx PDU, from 192.168.1.2:1800 to 192.168.1.254:54757 (26) PDU-dict=starent-vsa1
 Code: 41 (Disconnect-Ack)
 Id: 78
 Length: 26
 Authenticator: 34 84 5B 8E AF 02 1C F2 58 26 1B 0C 20 37 93 33
     Acct-Termination-Cause = Admin_Reset
```

El ID de bug de Cisco CSCuw78786 ha sido enviado. Esto se ha probado en la versión 17.2.0 y la versión 15.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).