Comprendere e risolvere i problemi relativi a RADIUS CoA e ai messaggi di disconnessione

Sommario

Introduzione

In questo documento vengono descritti i messaggi di disconnessione (DM) RADIUS.

Definizione dei messaggi RADIUS CoA

Un messaggio CoA (Change of Authorization) viene utilizzato per modificare gli attributi e i filtri dati associati a una sessione utente. Il sistema supporta i messaggi CoA provenienti dal server di autenticazione, autorizzazione e accounting (AAA) per modificare i filtri dati associati a una sessione sottoscrittore.

> **Nota:** I filtri negli attributi filter-id (se presenti nella richiesta) devono essere configurati in ASR 5000 per il traffico tra applicazione e utente. Questa è la forma degli Access Control Lists (ACL) e viene configurata in ASR 5000 con i comandi **ip access-list**.

Il messaggio di richiesta CoA deve contenere attributi per identificare la sessione utente; gli attributi e i filtri dati devono essere applicati alla sessione utente. L'attributo filter-id (ID attributo 11) contiene i nomi dei filtri. Se l'ASR 5000 esegue correttamente la richiesta CoA, un ACK CoA viene inviato al server RADIUS e i nuovi attributi e filtri dati vengono applicati alla sessione utente.

In caso contrario, viene inviato un NAK CoA con il motivo corretto come attributo di codice di errore senza apportare alcuna modifica alla sessione utente.

DM RADIUS

Il messaggio DM viene utilizzato per disconnettere le sessioni utente in ASR 5000 da un server RADIUS. Il messaggio di richiesta DM deve contenere gli attributi necessari per identificare la sessione utente. Se il sistema disconnette correttamente la sessione utente, DM ACK viene inviato nuovamente al server RADIUS. In caso contrario, DM-NAK viene inviato con le dovute motivazioni di errore.

Come accennato in precedenza, è possibile che il NAS non sia in grado di soddisfare i messaggi Disconnect-Request o CoA-Request per qualche motivo. L'attributo Error-Cause fornisce ulteriori dettagli sulla causa del problema. PUÒ essere incluso nei messaggi Disconnect-ACK, Disconnect-NAK e CoA-NAK.

Il campo Value (Valore) è costituito da quattro ottetti, contenenti un numero intero che specifica la causa dell'errore.

- I valori **0-199** e **300-399** sono riservati.
- I valori **200-299** indicano la riuscita dell'operazione, quindi è possibile inviare questi valori solo all'interno di un messaggio Disconnect-ACK o CoA-ACK e NON devono essere inviati all'interno di un messaggio Disconnect-NAK o CoA-NAK.
- I valori **400-499** rappresentano errori irreversibili commessi dal server RADIUS, in modo che POSSANO essere inviati nei messaggi CoA-NAK o Disconnect-NAK e NON DEVONO essere inviati nei messaggi CoA-ACK o Disconnect-ACK.
- I valori **500-599** rappresentano errori irreversibili che si verificano su un proxy NAS o RADIUS, in modo che POSSANO essere inviati all'interno di messaggi CoA-NAK e Disconnect-NAK, e NON DEVONO essere inviati all'interno di messaggi CoA-ACK o Disconnect-ACK. I valori relativi alla causa dell'errore DEVONO essere registrati dal server RADIUS.

I valori dei codici di errore (espressi in decimali) includono:

```
 #     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
```

Attributi per l'identificazione della sessione

Per identificare l'ASR 5000, è possibile utilizzare uno dei seguenti metodi:

- Indirizzo IP-NAS: L'indirizzo IP del NAS, se presente nella richiesta COA/DM, deve corrispondere all'indirizzo IP del NAS ASR 5000.
- Identificatore NAS: Se questo attributo è presente, il relativo valore deve corrispondere all'identificatore nas generato per la sessione utente.
  Questo è un attributo obbligatorio per l'identificazione della sessione, se ASR 5000 è configurato con NAS-Identifier.

Per identificare la sessione utente, viene utilizzato uno dei metodi seguenti:

- Account-Session-ID: Se questo attributo è presente, il relativo valore deve corrispondere all'acct-session-id per la sessione utente.
- Indirizzo IP con frame: Se questo attributo è presente, i relativi valori devono corrispondere all'indirizzo IP con frame della sessione.
- Username: Se questo attributo è presente, i relativi valori devono corrispondere al nome utente della sessione.
- Calling-Station-ID: Questa è l'identità IMSI (International Mobile Subscriber Identity) dell'utente.

Configurazione dei DM RADIUS

La configurazione di un DM RADIUS è abbastanza semplice. Tutte le linee devono essere configurate nel contesto di destinazione (quello con la configurazione RADIUS).

radius change-authorization-nas-ip *indirizzo_ip* **chiave [encrypted]** *valore* **[port** *port* **]**
[eventtimestamp-window *finestra* **] [no-nas-identification-check]**
[no-reverse-path-forward-check][input mpls-label *in_label_value* **| risultato** *out_label_value1*
[*out_label_value2* **]**

> **Nota:** Il valore "radius change-authorization-nas-ip" deve essere l'indirizzo di interfaccia AAA del contesto locale. questo comando CLI a volte può causare confusione.

Esempio di configurazione

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

Esempi di scenari di errore

Nessun messaggio DM ricevuto sul lato ASR 5000

Èpossibile che il socket non sia pronto per la porta UDP 3799. (In conformità alla RFC 3756, il

pacchetto RADIUS Disconnect-Request viene inviato alla porta UDP 3799).

Questo comportamento può essere semplificato. Il processo che gestisce tutte le richieste CoA è l'istanza di gestione 385, ovvero quella sulla scheda SMC/MIO attiva. Questo comando CLI deve essere eseguito nel contesto di destinazione.

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

Tale output avrà il seguente aspetto:

```
# 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
```

Nell'esempio, non è presente la porta 3799 e questa è la causa del comportamento segnalato. Se si verifica la stessa situazione, la soluzione è rimuovere e aggiungere nuovamente la configurazione CoA per ricreare il socket di ascolto. Inoltre, è possibile tentare di uccidere l'istanza 385 di amgr se la prima soluzione non aiuta.

Dopo le azioni descritte, verrà visualizzato questo output:

```
# 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
```

e il socket deve essere visibile dalla shell di debug sul contesto/VR appropriato:

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

Porta UDP 3379 con socket pronto senza messaggi DM

La porta UDP 3379 ha un socket pronto, ma i messaggi DM non vengono ancora visualizzati. Ciò è probabilmente causato da una configurazione errata di **radius change-authorization-nas-ip**. I valori degli attributi inclusi nel messaggio di richiesta DM non corrispondono a quelli inviati in una richiesta di accounting verso RADIUS.

Richiesta di accounting

```
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)
```

Disconnect-Request

```
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
```

Nell'esempio, il valore di **Acct-Session-Id** che arriva ad ASR 5000 è diverso da quello inviato verso RADIUS e questa è la causa del problema. Questo problema può essere risolto apportando modifiche appropriate sul lato RADIUS.

Èpossibile verificare l'account-Session-Id per la sessione attiva con il 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
```

Tutti gli attributi corrispondono, ma ASR 5000 invia a DM NAK il messaggio di errore: 401 - Attributo non supportato

A questo punto è noto che questo tipo di messaggio di errore indica che il problema proviene dal server RADIUS. Tuttavia, non è ancora chiaro cosa sia sbagliato. In questo caso, la limitazione di ASR 5000 non supporta l'ID stazione chiamata in Radius DM. Quindi, se viene visualizzata, risponde con l'errore evidenziato.

```
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)
```

Il sistema ha configurato "no-nas-identification-check" nella riga "radius change-authorization-nas-ip". Errore "NAS-Identification-Mismatch" ancora restituito

Ciò si verifica nella configurazione seguente:

```
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
```

Per un contesto PDP attivo, la richiesta di disconnessione è NAK:

```
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)
```

Tuttavia, quando questa riga è inclusa nel gruppo AAA predefinito:

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

comincia a funzionare:

```
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
```

Oppure funzionerà anche senza la configurazione dell'identificatore-nas sul gruppo AAA, ma con l'AVP dell'identificatore-NAS rimosso da Disconnect-Request:

```
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
```

L'ID bug Cisco CSCuw78786 è stato inviato. Questo è stato testato sulle release 17.2.0 e 15.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).