

瞭解並排除RADIUS CoA和斷開連線消息故障

目錄

[簡介](#)

[RADIUS CoA訊息的定義](#)

[RADIUS DM](#)

[會話標識的屬性](#)

[RADIUS DM的配置](#)

[示例配置](#)

[故障方案示例](#)

[ASR 5000端未收到DM消息](#)

[UDP埠3379有現成的套接字，沒有DM消息](#)

[記帳請求](#)

[Disconnect-Request](#)

[所有屬性都匹配，但ASR 5000會傳送DM NAK並顯示以下錯誤消息：401 — 不支援的屬性](#)

[系統已在「radius change-authorize-nas-ip」行中配置「no-nas-identification-check」，「NAS-Identification-Mismatch」錯誤仍返回](#)

簡介

本檔案將說明RADIUS結束通話訊息(DM)。

RADIUS CoA訊息的定義

使用授權變更(CoA)消息來變更與使用者會話相關聯的屬性和資料過濾器。系統支援來自身份驗證、授權和記帳(AAA)伺服器的CoA消息以更改與使用者會話關聯的資料過濾器。

附註：應在ASR 5000中配置filter-id屬性中的過濾器（如果請求中存在），以便應用於使用者流量。這是訪問控制清單(ACL)的形式，並使用ip access-list命令在ASR 5000中配置。

CoA請求消息應包含用於標識使用者會話的屬性；需要將屬性和資料過濾器應用到使用者會話。filter-id屬性（屬性id 11）包含過濾器的名稱。如果ASR 5000成功執行CoA請求，則會將CoA ACK傳送回RADIUS伺服器，並將新的屬性和資料過濾器應用到使用者會話。否則，將以正確原因傳送CoA NAK作為錯誤代碼屬性，而不對使用者會話進行任何更改。

RADIUS DM

DM消息用於從RADIUS伺服器斷開ASR 5000中的使用者會話。DM請求消息應包含識別使用者會話

所需的屬性。如果系統成功斷開使用者會話，則DM ACK將傳送回RADIUS伺服器。否則，傳送DM-NAK時會顯示正確的錯誤原因。

如前所述，由於某種原因，NAS可能無法承受Disconnect-Request或CoA-Request消息。「錯誤原因」屬性提供了有關問題原因的更多詳細資訊。它可以包含在Disconnect-ACK、Disconnect-NAK和CoA-NAK消息中。

「值」欄位為四個八位數，其中包含指定錯誤原因的整數。

- 保留值0-199和300-399。
- 200-299值表示成功完成，因此這些值可能只在Disconnect-ACK或CoA-ACK消息中傳送，不能在Disconnect-NAK或CoA-NAK中傳送。
- 值400-499表示RADIUS伺服器提交的致命錯誤，以便可以在CoA-NAK或Disconnect-NAK消息中傳送這些錯誤，且不得在CoA-ACK或Disconnect-ACK消息中傳送這些錯誤。
- 值500-599表示NAS或RADIUS代理上發生的致命錯誤，以便可以在CoA-NAK和Disconnect-NAK消息中傳送這些錯誤，而且不得在CoA-ACK或Disconnect-ACK消息中傳送這些錯誤。錯誤原因值應該由RADIUS伺服器記錄。

錯誤代碼值（以十進位制表示）包括：

#	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

會話標識的屬性

要識別ASR 5000，可以使用以下方法之一：

- NAS-IP-Address:NAS IP地址（如果存在COA/DM請求中）應與ASR 5000 NAS IP地址匹配。
- NAS識別符號：如果存在此屬性，則其值應與為使用者會話生成的nas識別符號相匹配。如果ASR 5000配置了NAS-Identifier，這是會話標識的強制屬性。

為了標識使用者會話，可以使用以下方法之一：

- Acct-Session-ID:如果存在此屬性，則其值應與使用者會話的acct-session-id匹配。
- Framed-IP-Address:如果存在此屬性，則其值應與會話的框架化IP地址匹配。
- 使用者名稱:如果存在此屬性，則其值應與會話的使用者名稱匹配。
- Calling-Station-ID:這是使用者的國際移動使用者身份(IMSIs)。

RADIUS DM的配置

RADIUS DM的設定非常容易。所有線路都需要配置在目標環境中（具有RADIUS配置的線路）。

```
radius change-authorize-nas-ip ip_address [ encrypted ]金鑰 價值 [連接埠 連接埠 ]  
[ eventtimestamp-window 視窗 ] [ no-nas-identification-check ]  
[ no-reverse-path-forward-check][ mpls標籤輸入 in_label_value |輸出 out_label_value1  
[ out_label_value2 ]
```

附註：「radius change-authorize-nas-ip」應該是本地環境的AAA介面地址。此CLI命令有時會引起混淆。

示例配置

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

故障方案示例

ASR 5000端未收到DM消息

可能套接字尚未為UDP埠3799做好準備。（根據RFC 3756,RADIUS斷開請求資料包將傳送到UDP埠3799）。

此行為可以簡化。處理所有CoA請求的流程是aamgr例項385，它是活動SMC/MIO卡上的例項。需要在目標上下文中執行此CLI命令。

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

此類輸出如下所示：

```
# 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
```

在本範例中，沒有連線埠3799，這是報告行為的原因。如果您在案例中看到相同的情況，解決方案是刪除並重新新增CoA配置，以便重新建立偵聽套接字。此外，如果第一個解決方案不起作用，您可以嘗試停止生成例項385。

執行上述操作後，您應該會看到以下輸出：

```
# 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
```

而且套接字應該可以從相應上下文/VR上的調試外殼中看到：

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

UDP埠3379有現成的套接字，沒有DM消息

UDP埠3379有現成的套接字，但是您仍然看不到DM消息。這可能是由於radius change-authorize-nas-ip組態錯誤所造成。DM請求消息中的屬性值與在Accounting請求中向RADIUS傳送的屬性值不匹配。

記帳請求

```
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

```

在本示例中，指向ASR 5000的**Acct-Session-Id**值與傳送到RADIUS的值不同，這是出現問題的原因。此問題可通過在RADIUS端進行適當的更改來解決。

可以使用**show subscribers ggsn-only aaa-configuration active imsi <>**命令驗證活動會話的Acct-Session-Id。

```

[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

```

所有屬性都匹配，但ASR 5000會傳送DM NAK並顯示以下錯誤消息：401 — 不支援的屬性

目前已知這種錯誤訊息表示問題來自RADIUS伺服器。然而，目前仍不清楚問題出在哪裡。這裡，ASR 5000的限制不支援Radius DM中的Called-station-Id。因此，如果它出現在此處，則會以突出顯示的錯誤來回答。

```

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

```


Value: 00 00 01 93
(NAS-Identification-Mismatch)

但是，當此行包含在預設AAA組中時：

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

它開始發揮作用：

```
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-vs1
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-vs1
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
```

或者，它也可以不在AAA組上配置nas-identifier，但從Disconnect-Request中刪除NAS-Identifier AVP的情況下工作：

```
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-vs1
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-vs1
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
```

思科錯誤ID [CSCuw78786](#)已提交。已在17.2.0版和15版上測試此功能。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。