

Begrijp en los problemen op met RADIUS CoA en verbreek berichten

Inhoud

[Inleiding](#)

[Definitie van RADIUS CoA-berichten](#)

[RADIUS-DM](#)

[Attributen voor Session Identification](#)

[Configuratie van RADIUS-DM's](#)

[Voorbeeldconfiguratie](#)

[Scenario-voorbeelden van fouten](#)

[Geen DM-berichten ontvangen aan de ASR 5000-zijde](#)

[UDP-poort 3379 heeft kant-en-klare socket zonder DM-berichten](#)

[Boekhoudkundige aanvraag](#)

[Aanvraag voor verbinding verbreken](#)

[Alle kenmerken komen overeen, maar de ASR 5000 verzendt DM NAK met de foutmelding: 401 - Niet-ondersteunde kenmerk](#)

[System heeft geconfigureerd "no-nas-identifier-check" in de "radius verandering-autorisatie-nas-ip"-lijn, "NAS-Identification-Mismatch"-fout nog steeds teruggestuurd](#)

Inleiding

Dit document beschrijft RADIUS-ontkoppelingsberichten (DM's).

Definitie van RADIUS CoA-berichten

Een bericht Wijziging van autorisatie (CoA) wordt gebruikt om kenmerken en gegevensfilters die bij een gebruikerssessie horen, te wijzigen. Het systeem ondersteunt CoA-berichten van de AAA-server (Verificatie, autorisatie en accounting) om gegevensfilters te wijzigen die gekoppeld zijn aan een abonneesessie.

Opmerking: de filters in filter-id-kenmerken (indien aanwezig in het verzoek) moeten in de ASR 5000 worden geconfigureerd voor toepassing op het gebruikersverkeer. Dit is de vorm van toegangscontrolelijsten (ACL's) en wordt in de ASR 5000 geconfigureerd met **IP-toegangslijsten**.

Het bericht van de CoA-aanvraag moet kenmerken bevatten om de gebruikerssessie te identificeren; kenmerken en gegevensfilters moeten op de gebruikerssessie worden toegepast. Het kenmerk filter-id (kenmerk id 11) bevat de namen van de filters. Als de ASR 5000 het verzoek

van de CoA met succes uitvoert, wordt een CoA-ACK teruggestuurd naar de RADIUS-server en worden de nieuwe attributen en gegevensfilters toegepast op de gebruikerssessie. Anders wordt een CoA NAK met de juiste reden verzonden als een fout-code attribuut zonder enige veranderingen aan de gebruikerssessie aan te brengen.

RADIUS-DM

Het DM-bericht wordt gebruikt om de gebruikerssessies in de ASR 5000 los te koppelen van een RADIUS-server. Het DM-verzoekbericht dient de nodige kenmerken te bevatten om de gebruikerssessie te kunnen identificeren. Als het systeem de gebruikerssessie succesvol afsluit, wordt DM ACK teruggestuurd naar de RADIUS-server. Anders, wordt DM-NAK verzonden met juiste foutenredenen.

Zoals eerder vermeld, is het mogelijk dat de NAS om een of andere reden niet kan voldoen aan de berichten van het verzoek om verbinding verbreken of CoA-verzoek. Het kenmerk Fout-Oorzaak biedt meer details over de oorzaak van het probleem. Het KAN worden opgenomen in Disconnect-ACK, Disconnect-NAK en CoA-NAK berichten.

Het veld Waarde bestaat uit vier octetten. Dit veld bevat een geheel getal dat de oorzaak van de fout aangeeft.

- De waarden **0-199** en **300-399** zijn gereserveerd.
- De waarden **200-299** vertegenwoordigen een succesvolle voltooiing, zodat deze waarden alleen kunnen worden verzonden binnen een Disconnect-ACK of CoA-ACK bericht en NIET MOGEN worden verzonden binnen een Disconnect-NAK of CoA-NAK.
- De waarden **400-499** vertegenwoordigen fatale fouten die door de RADIUS-server zijn gemaakt, zodat ze kunnen worden verzonden binnen CoA-NAK- of Disconnect-NAK-berichten en NIET mogen worden verzonden binnen CoA-ACK- of Disconnect-ACK-berichten.
- Waarden **500-599** vertegenwoordigen fatale fouten die voorkomen op een NAS of RADIUS proxy, zodat ze KUNNEN worden verzonden binnen CoA-NAK en loskoppelen-NAK berichten, en MOGEN NIET worden verzonden binnen CoA-ACK of loskoppelen-ACK berichten. Error-Cause waarden DIENEN te worden vastgelegd op de RADIUS-server.

De waarden van de fout-code (die in decimaal worden uitgedrukt) omvatten:

#	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

Attributen voor Session Identification

Voor de identificatie van de ASR 5000 kan een van deze methoden worden gebruikt:

- NAS-IP-adres: NAS IP-adres indien aanwezig in het COA/DM-verzoek moet overeenkomen met het ASR 5000 NAS IP-adres.
- NAS-Identificatie: Als deze eigenschap aanwezig is, moet de waarde overeenkomen met de nas-identificatie die voor de gebruikerssessie is gegenereerd.
Dit is een verplicht kenmerk voor sessie-identificatie, als de ASR 5000 is geconfigureerd met NAS-Identificatie.

Voor identificatie van de gebruikerssessie wordt een van deze methoden gebruikt:

- Acct-Session-ID: Als deze eigenschap aanwezig is, moet de waarde overeenkomen met de acct-sessie-id voor de gebruikerssessie.
- Framed-IP-Address: Als deze eigenschap aanwezig is, moeten de waarden overeenkomen met het framed IP-adres van de sessie.
- Gebruikersnaam: Als deze eigenschap aanwezig is, moeten de waarden overeenkomen met de gebruikersnaam van de sessie.
- Calling-Station-ID: Dit is de International Mobile Subscriber Identity (IMSI) van de gebruiker.

Configuratie van RADIUS-DM's

De configuratie van een RADIUS-DM is vrij eenvoudig. Alle lijnen moeten in doelcontext worden geconfigureerd (de met de RADIUS-configuratie).

```
radiuswijziging-autorisatie-nas-ip IP-adres [ versleuteld ] toets waarde [ port port ]  
[ eventtimestamp-venster vensterruit ] [ geen-nas-identificatiecontrole ]  
[ niet-omgekeerde weg-voorwaartse controle ] [ mpls-label invoer in_label_waarde ] output  
out_label_waarde1  
[ out_label_waarde2 ]
```

Opmerking: de "radius change-authorized-nas-ip" moet het AAA-interfaceadres van uw lokale context zijn. Deze CLI opdracht is soms een bron van verwarring.

Voorbeeldconfiguratie

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

Scenario-voorbeelden van fouten

Geen DM-berichten ontvangen aan de ASR 5000-zijde

Het is mogelijk dat de socket niet klaar is voor UDP-poort 3799. (In overeenstemming met RFC 3756 wordt het RADIUS-pakket voor loskoppeling naar UDP-poort 3799 verzonden).

Dit gedrag kan worden vereenvoudigd. Het proces dat alle CoA-verzoeken behandelt, is bijvoorbeeld 385, dat is het proces op de actieve SMC/MIO-kaart. Dit CLI-commando moet worden uitgevoerd in de doelcontext.

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

Zulke output ziet er als volgt uit:

```
# 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
```

In dit voorbeeld is er geen poort 3799 en dit is de reden voor het gerapporteerde gedrag. Als u hetzelfde ziet in uw geval, is de oplossing om de CoA configuratie te verwijderen en opnieuw toe te voegen om de luistersocket te herscheppen. Daarnaast kunt u proberen om amgr instantie 385 te doden als de eerste oplossing niet helpt.

Na de beschreven acties ziet u deze uitvoer:

```
# 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
```

en de socket moet zichtbaar zijn vanuit de debug shell op de juiste context/VR:

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

UDP-poort 3379 heeft kant-en-klare socket zonder DM-berichten

De UDP-poort 3379 heeft een kant-en-klare aansluiting, maar de DM-berichten worden nog steeds niet weergegeven. Dit wordt waarschijnlijk veroorzaakt door een onjuiste configuratie van **radiuswijziging-autorisatie-nas-ip**. Ofwel de attribuuwaarden die in het DM-verzoekbericht zijn

opgenomen, komen niet overeen met de waarden die in een boekhoudkundige aanvraag naar RADIUS zijn verzonden.

Boekhoudkundige aanvraag

```
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)
```

Aanvraag voor verbinding verbreken

```
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
```

In dit voorbeeld is de waarde van **Acct-Session-ID** die naar de ASR 5000 komt, anders dan die naar RADIUS gestuurd wordt en dit is de reden voor het probleem. Dit probleem kan door juiste veranderingen aan de kant van de RADIUS worden opgelost.

De Acct-Session-ID voor de actieve sessie kan worden geverifieerd met de opdracht **toont abonnees ggsn-only aaa-configuratie actieve 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

Alle kenmerken komen overeen, maar de ASR 5000 verzendt DM NAK met de foutmelding: 401 - Niet-ondersteunde kenmerk

Op dit punt is bekend dat dit soort foutmelding betekent dat het probleem afkomstig is van de RADIUS-server. Het is echter nog steeds niet duidelijk wat er mis is. Op dit punt ondersteunt de beperking van de ASR 5000 geen Call-Station-ID in Radius DM. Als je het daar ziet, antwoordt het met de gemarkeerde fout.

```
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)
```

System heeft geconfigureerd "no-nas-identifier-check" in de "radius verandering-autorisatie-nas-ip"-lijn, "NAS-Identification-Mismatch"-fout nog steeds teruggestuurd

Dit gebeurt in deze configuratie:

```
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
```

Voor een actieve PDP-context is de aanvraag voor verbinding verbreken 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-vs1
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)
&nbsp; 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-vs1
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)
```

Wanneer deze regel echter is opgenomen in de standaard AAA-groep:

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

zij begint te werken:

```
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**

Of het werkt ook zonder configuratie van de nas-identificer op de AAA-groep, maar met NAS-Identificer AVP verwijderd uit de 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-vsai

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-vsai

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**

Cisco bug-id [CSCuw78786](#) is ingediend. Dit is getest op release 17.2.0 en release 15.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.