

RADIUS-CoA- und Trennungsmeldungen verstehen und Fehler beheben

Inhalt

[Einleitung](#)

[Definition von RADIUS-CoA-Meldungen](#)

[RADIUS-DM](#)

[Attribute für die Sitzungserkennung](#)

[Konfiguration von RADIUS-DMs](#)

[Konfigurationsbeispiel](#)

[Beispiele für Fehlerszenarien](#)

[Keine DM-Nachrichten auf Seite des ASR 5000 empfangen](#)

[UDP-Port 3379 verfügt über einen Socket ohne DM-Nachrichten](#)

[Buchungsanfrage](#)

[Verbindungstrennung](#)

[Alle Attribute stimmen überein, aber der ASR 5000 sendet DM NAK mit der Fehlermeldung: 401 - Unsupported Attribute \(Nicht unterstütztes Attribut\)](#)

[System hat "no-nas-identification-check" in der Zeile "radius change-Authorize-nas-ip" konfiguriert, Fehler "NAS-Identification-Mismatch" wird weiterhin ausgegeben](#)

Einleitung

In diesem Dokument werden RADIUS-Trennungsmeldungen (Disconnect Messages, DMs) beschrieben.

Definition von RADIUS-CoA-Meldungen

Eine Autorisierungsänderungsmeldung (Change of Authorization, CoA) dient zum Ändern von Attributen und Datenfiltern, die einer Benutzersitzung zugeordnet sind. Das System unterstützt CoA-Meldungen vom AAA-Server (Authentication, Authorization, and Accounting), um die Datenfilter einer Teilnehmersitzung zu ändern.

Hinweis: Die Filter in den Filtern-ID-Attributen (sofern in der Anforderung vorhanden) sollten im ASR 5000 für den Datenverkehr der Benutzer konfiguriert werden. Dies ist die Form von Zugriffskontrolllisten (Access Control Lists, ACLs) und wird im ASR 5000 mit **IP-Zugriffslisten**-Befehlen konfiguriert.

Die CoA-Anforderungsmeldung sollte Attribute zur Identifizierung der Benutzersitzung enthalten. Attribute und Datenfilter müssen auf die Benutzersitzung angewendet werden. Das Attribut filter-id

(Attribut id 11) enthält die Namen der Filter. Wenn der ASR 5000 die CoA-Anforderung erfolgreich ausführt, wird ein CoA ACK an den RADIUS-Server zurückgesendet, und die neuen Attribute und Datenfilter werden auf die Benutzersitzung angewendet. Andernfalls wird ein CoA-NAK mit dem richtigen Grund als Fehlercodeattribut gesendet, ohne dass Änderungen an der Benutzersitzung vorgenommen werden.

RADIUS-DM

Die DM-Nachricht wird verwendet, um Benutzersitzungen im ASR 5000 von einem RADIUS-Server zu trennen. Die DM-Anforderungsnachricht sollte die notwendigen Attribute enthalten, um die Benutzersitzung zu identifizieren. Wenn das System die Benutzersitzung erfolgreich trennt, wird DM ACK an den RADIUS-Server zurückgesendet. Andernfalls wird DM-NAK mit den richtigen Fehlergründen gesendet.

Wie bereits erwähnt, ist es möglich, dass das NAS aus irgendeinem Grund Disconnect-Request- oder CoA-Request-Meldungen nicht berücksichtigen kann. Das Error-Cause-Attribut enthält weitere Informationen zur Ursache des Problems. Sie KANN in Disconnect-ACK-, Disconnect-NAK- und CoA-NAK-Nachrichten enthalten sein.

Das Feld Wert umfasst vier Oktette. Es enthält eine ganze Zahl, die die Ursache des Fehlers angibt.

- Die Werte **0-199** und **300-399** sind reserviert.
- Die Werte **200-299** stellen einen erfolgreichen Abschluss dar, sodass diese Werte nur in der Disconnect-ACK- oder CoA-ACK-Nachricht gesendet werden können und NICHT innerhalb eines Disconnect-NAK oder CoA-NAK gesendet werden DÜRFEN.
- Die Werte **400-499** stellen schwerwiegende Fehler dar, die vom RADIUS-Server gemeldet wurden, sodass sie in CoA-NAK- oder Disconnect-NAK-Nachrichten gesendet werden KÖNNEN und NICHT in CoA-ACK- oder Disconnect-ACK-Nachrichten gesendet werden DÜRFEN.
- Die Werte **500-599** stellen schwerwiegende Fehler dar, die auf einem NAS- oder RADIUS-Proxy auftreten, sodass sie in CoA-NAK- und Disconnect-NAK-Nachrichten gesendet werden KÖNNEN und NICHT in CoA-ACK- oder Disconnect-ACK-Nachrichten gesendet werden DÜRFEN. Error-Cause-Werte MÜSSEN vom RADIUS-Server protokolliert werden.

Zu den Fehlercodewerten (in Dezimalzahlen ausgedrückt) gehören:

#	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

Attribute für die Sitzungserkennung

Zur Identifizierung des ASR 5000 kann eine der folgenden Methoden verwendet werden:

- **NAS-IP-Adresse:** Die NAS-IP-Adresse, falls in der COA/DM-Anfrage vorhanden, muss mit der NAS-IP-Adresse des ASR 5000 übereinstimmen.
- **NAS-Identifizierer:** Wenn dieses Attribut vorhanden ist, sollte sein Wert mit dem für die Benutzersitzung generierten NAS-Identifizierer übereinstimmen.
Dies ist ein obligatorisches Attribut für die Sitzungsidentifizierung, wenn der ASR 5000 mit NAS-Identifizierer konfiguriert ist.

Zur Identifizierung der Benutzersitzung wird eine der folgenden Methoden verwendet:

- **Account-Session-ID:** Wenn dieses Attribut vorhanden ist, muss sein Wert mit der acct-session-id für die Benutzersitzung übereinstimmen.
- **Framed-IP-Adresse:** Wenn dieses Attribut vorhanden ist, müssen seine Werte mit der gerahmten IP-Adresse der Sitzung übereinstimmen.
- **Benutzername:** Wenn dieses Attribut vorhanden ist, müssen seine Werte mit dem Benutzernamen der Sitzung übereinstimmen.
- **Calling-Station-ID:** Dies ist die Internationale Mobilfunk-Teilnehmerkennung (IMSI) des Benutzers.

Konfiguration von RADIUS-DMs

Die Konfiguration eines RADIUS DM ist ganz einfach. Alle Leitungen müssen im Zielkontext (der mit der RADIUS-Konfiguration) konfiguriert werden.

```
radius change-authorize-nas-ip IP-Adresse [ verschlüsselter ] Schlüssel wert [anschluss  
anschluss ]  
[ eventTimestamp-window Fenster ] [ no-nas-identification-check ]  
[ no-reverse-path-forward-check ] [ MPLS-Label-Eingabe in_label_value | Ausgabe  
out_label_value1  
[ out_label_value2 ]
```

Hinweis: Bei der Option "radius change-authorize-nas-ip" sollte es sich um die AAA-Schnittstellenadresse des lokalen Kontexts handeln. Dieser CLI-Befehl kann zu Verwirrung führen.

Konfigurationsbeispiel

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

Beispiele für Fehlerszenarien

Keine DM-Nachrichten auf Seite des ASR 5000 empfangen

Möglicherweise ist der Socket nicht bereit für den UDP-Port 3799. (Gemäß RFC 3756 wird das RADIUS Disconnect-Request-Paket an den UDP-Port 3799 gesendet.)

Dieses Verhalten kann vereinfacht werden. Der Prozess, der alle CoA-Anfragen verarbeitet, ist die Aamgr-Instanz 385, die auf der aktiven SMC/MIO-Karte vorhanden ist. Dieser CLI-Befehl muss im Zielkontext ausgeführt werden.

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

Diese Ausgabe sieht wie folgt aus:

```
# 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 diesem Beispiel gibt es keinen Port 3799, und dies ist der Grund für das gemeldete Verhalten. Wenn in Ihrem Fall das Gleiche geschieht, können Sie die CoA-Konfiguration entfernen und erneut hinzufügen, um den Listening-Socket neu zu erstellen. Zusätzlich können Sie versuchen, aamgr Instanz 385 zu töten, wenn die erste Lösung nicht hilft.

Nach den beschriebenen Aktionen sollten Sie die folgende Ausgabe sehen:

```
# 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
```

und der Socket sollte in der Debug-Shell im entsprechenden Kontext/VR sichtbar sein:

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

UDP-Port 3379 verfügt über einen Socket ohne DM-Nachrichten

Der UDP-Port 3379 verfügt über einen Socket-Vorlauf, die DM-Meldungen werden jedoch weiterhin nicht angezeigt. Dies ist wahrscheinlich auf eine falsche Konfiguration von **radius change-authorize-nas-ip** zurückzuführen. Entweder stimmen die Attributwerte in der DM-Anforderungsnachricht nicht mit den Attributwerten überein, die in einer Accounting-Anforderung an RADIUS gesendet wurden.

Buchungsanfrage

```
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)
```

Verbindungstrennung

```
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 diesem Beispiel unterscheidet sich der Wert von "**Account-Session-Id**" für den ASR 5000 von dem Wert, der an RADIUS gesendet wird. Dies ist der Grund für das Problem. Dieses Problem kann durch entsprechende RADIUS-Änderungen behoben werden.

Die Acct-Session-Id für die aktive Sitzung kann mit dem Befehl **show subscribers ggsn-only aaa-**

configuration active imsi <> überprüft werden.

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

```
Username: 998931720911@mihcl          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 Attribute stimmen überein, aber der ASR 5000 sendet DM NAK mit der Fehlermeldung: 401 - Unsupported Attribute (Nicht unterstütztes Attribut)

An dieser Stelle ist bekannt, dass diese Art von Fehlermeldung bedeutet, dass das Problem vom RADIUS-Server stammt. Es ist jedoch immer noch nicht klar, was falsch ist. In diesem Fall unterstützt die Beschränkung des ASR 5000 die Called-Station-Id in Radius DM nicht. Wenn sie dort angezeigt wird, wird sie mit dem hervorgehobenen Fehler beantwortet.

```
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-Identifizier)
    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 hat "no-nas-identification-check" in der Zeile "radius change-Authorize-nas-ip" konfiguriert, Fehler "NAS-Identification-Mismatch" wird weiterhin ausgegeben

Dies geschieht in dieser Konfiguration:

```
radius change-authorize-nas-ip 192.168.1.2 encrypted key
+A27wvxlgY06ia30pcqswmdajxd11ckg4ns88i6192dghsqw7v77f1 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
```

Für einen aktiven PDP-Kontext lautet die Trennungsanforderung 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;nbsp;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)
```

Wenn dieser Posten jedoch in der AAA-Standardgruppe enthalten ist, gilt Folgendes:

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

funktioniert es:

```
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**

Oder es funktioniert auch ohne Konfiguration des NAS-Identifizierers auf der AAA-Gruppe, aber mit NAS-Identifizierer AVP aus der Disconnect-Anforderung entfernt:

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**

Cisco Bug-ID [CSCuw78786](#) wurde übermittelt. Dies wurde in Version 17.2.0 und Version 15 getestet.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.