

RADIUS CoA 및 연결 끊기 메시지 이해 및 문제 해결

목차

[소개](#)

[RADIUS CoA 메시지 정의](#)

[RADIUS DM](#)

[세션 ID의 특성](#)

[RADIUS DM 컨피그레이션](#)

[샘플 설정](#)

[실패 시나리오 예](#)

[ASR 5000 측에서 수신된 DM 메시지가 없음](#)

[UDP 포트 3379에 DM 메시지 없이 준비된 소켓](#)

[회계 요청](#)

[연결 해제 요청](#)

[모든 특성이 일치하지만 ASR 5000이 DM NAK에 오류 메시지 401 - Unsupported Attribute\(지원되지 않는 특성\)를 보냅니다.](#)

[시스템에서 "radius change-authorize-nas-ip" 줄에 "no-nas-identification-check"를 구성했습니다.](#)

["NAS-Identification-Mismatch" 오류가 계속 반환되었습니다.](#)

소개

이 문서에서는 RADIUS 연결 해제 메시지(DM)에 대해 설명합니다.

RADIUS CoA 메시지 정의

CoA(Change of Authorization) 메시지는 사용자 세션과 연결된 특성 및 데이터 필터를 변경하는 데 사용됩니다. 시스템은 AAA(Authentication, Authorization, and Accounting) 서버의 CoA 메시지를 지원하여 가입자 세션과 연결된 데이터 필터를 변경합니다.

참고: 사용자 트래픽에 적용하려면 filter-id 특성의 필터(요청에 있는 경우)를 ASR 5000에서 구성해야 합니다. 이는 ACL(Access Control Lists)의 형태이며 ASR 5000에서 ip access-list 명령을 사용하여 구성됩니다.

CoA 요청 메시지에는 사용자 세션을 식별하는 특성이 포함되어야 합니다. 특성과 데이터 필터는 사용자 세션에 적용되어야 합니다. filter-id 특성(특성 id 11)에는 필터 이름이 포함되어 있습니다. ASR 5000이 CoA 요청을 성공적으로 실행하면 CoA ACK가 RADIUS 서버로 다시 전송되고 새 특성 및 데이터 필터가 사용자 세션에 적용됩니다. 그렇지 않은 경우 CoA NAK는 사용자 세션을 변경하지 않고 적절한 이유를 오류 코드 특성으로 전송합니다.

RADIUS DM

DM 메시지는 RADIUS 서버에서 ASR 5000의 사용자 세션 연결을 끊는 데 사용됩니다. DM 요청 메시지는 사용자 세션을 식별하기 위해 필요한 속성을 포함해야 합니다. 시스템이 사용자 세션의 연결을 성공적으로 끊으면 DM ACK가 RADIUS 서버로 다시 전송됩니다. 그렇지 않으면 DM-NAK가 적절한 오류 이유와 함께 전송됩니다.

앞서 언급한 것처럼, NAS에서 어떤 이유로든 Disconnect-Request 또는 CoA-Request 메시지를 수락하지 않을 수 있습니다. Error-Cause Attribute는 문제의 원인에 대한 자세한 정보를 제공합니다. Disconnect-ACK, Disconnect-NAK 및 CoA-NAK 메시지에 포함될 수 있습니다.

Value 필드는 4개의 옥텟으로, 오류의 원인을 지정하는 정수가 들어 있습니다.

- 값 0-199 및 300-399는 예약되어 있습니다.
- 값 200-299는 성공적인 완료를 나타내므로 이러한 값은 Disconnect-ACK 또는 CoA-ACK 메시지 내에서만 전송될 수 있으며 Disconnect-NAK 또는 CoA-NAK 내에서는 전송되어서는 안 됩니다.
- 값 400-499는 RADIUS 서버에서 커밋한 치명적인 오류를 나타내며, 이는 CoA-NAK 또는 Disconnect-NAK 메시지 내에서 전송될 수 있고 CoA-ACK 또는 Disconnect-ACK 메시지 내에서 전송되어서는 안 됩니다.
- 값 500-599는 NAS 또는 RADIUS 프록시에서 발생하는 치명적인 오류를 나타내며, CoA-NAK 및 Disconnect-NAK 메시지 내에서 전송될 수 있으며 CoA-ACK 또는 Disconnect-ACK 메시지 내에서 전송되어서는 안 됩니다. 오류-원인 값은 RADIUS 서버에 의해 기록되어야 합니다.

오류 코드 값(십진수로 표시됨)은 다음과 같습니다.

#	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

세션 ID의 특성

ASR 5000을 식별하기 위해 다음 방법 중 하나를 사용할 수 있습니다.

- NAS-IP-Address: NAS IP 주소(COA/DM 요청에 있는 경우)는 ASR 5000 NAS IP 주소와 일치해야 합니다.
- NAS-Identifier: 이 특성이 있는 경우 해당 값은 사용자 세션에 대해 생성된 nas-identifier와 일치해야 합니다.
ASR 5000이 NAS 식별자로 구성된 경우 세션 식별을 위한 필수 속성입니다.

사용자 세션을 식별하기 위해 다음 방법 중 하나를 사용합니다.

- Acct-Session-ID: 이 특성이 있는 경우 해당 값은 사용자 세션의 acct-session-id와 일치해야 합니다.
- Framed-IP-Address: 이 특성이 있는 경우 해당 값은 세션의 framed IP 주소와 일치해야 합니다.
- 사용자 이름: 이 특성이 있는 경우 해당 값은 세션의 사용자 이름과 일치해야 합니다.
- Calling-Station-ID: 사용자의 국제 모바일 가입자 ID(IMSI)입니다.

RADIUS DM 컨피그레이션

RADIUS DM의 컨피그레이션은 매우 쉽습니다. 모든 라인은 대상 컨텍스트(RADIUS 컨피그레이션이 있는 라인)에서 구성해야 합니다.

```
radius change-authorize-nas-ip ip_주소 [ encrypted ] 키 값 [포트 포트 ]
[ eventtimestamp-window 창 ] [ no-nas-identification-check ]
[ no-reverse-path-forward-check][ mpls-label input in_label_value | 성과 out_label_value1
[ out_label_value2 ]
```

참고: "radius change-authorize-nas-ip"는 로컬 컨텍스트의 AAA 인터페이스 주소여야 합니다. 이 CLI 명령은 때때로 혼동의 원인입니다.

샘플 설정

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

실패 시나리오 예

ASR 5000 측에서 수신된 DM 메시지가 없음

소켓이 UDP 포트 3799에 대해 준비되지 않았을 수 있습니다. (RFC 3756에 따라 RADIUS Disconnect-Request 패킷이 UDP 포트 3799로 전송됩니다.)

이러한 동작을 간소화할 수 있습니다. 모든 CoA 요청을 처리하는 프로세스는 활성 SMC/MIO 카드에 있는 AAAMGR 인스턴스 385입니다. 이 CLI 명령은 대상 컨텍스트에서 실행해야 합니다.

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

이러한 출력은 다음과 같습니다.

```
<#root>
#
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
```

이 예에서는 포트 3799가 없으며 이것이 보고된 동작의 이유입니다. 이 경우 동일한 항목이 표시되면 해결 방법은 수신 소켓을 다시 생성하기 위해 CoA 컨피그레이션을 제거하고 다시 추가하는 것입니다. 또한 첫 번째 솔루션이 도움이 되지 않으면 aaamgr 인스턴스 385를 종료하려고 시도할 수 있습니다.

설명된 작업 후 다음 출력이 표시되어야 합니다.

```
<#root>
#
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
```

그리고 소켓은 해당 컨텍스트/VR의 디버그 셸에서 볼 수 있어야 합니다.

<#root>

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

UDP 포트 3379에 DM 메시지 없이 준비된 소켓

UDP 포트 3379에 소켓이 준비되었지만 여전히 DM 메시지가 표시되지 않습니다. 이는 아마도 radius change-authorize-nas-ip의 잘못된 컨피그레이션으로 인해 발생할 수 있습니다. DM 요청 메시지에 있는 특성 값이 RADIUS에 대한 어카운팅 요청에서 전송된 값과 일치하지 않습니다.

회계 요청

<#root>

```
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 0603A2
BF
      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)
```

연결 해제 요청

<#root>

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

```
: BC71DF260603A2
```

00

이 예에서 ASR 5000에 제공되는 Acct-Session-Id의 값이 RADIUS로 전송되는 값과 다르며 이것이 문제의 원인입니다. 이 문제는 RADIUS 측에서 적절하게 변경하여 해결할 수 있습니다.

활성 세션에 대한 Acct-Session-Id는 show subscribers ggsn-only aaa-configuration active imsi <> 명령을 사용하여 확인할 수 있습니다.

<#root>

[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

모든 특성이 일치하지만 ASR 5000이 DM NAK에 오류 메시지 401 - Unsupported Attribute(지원되지 않는 특성)를 보냅니다.

이 시점에서 이러한 유형의 오류 메시지는 RADIUS 서버에서 문제가 발생한다는 것을 의미합니다. 하지만 무엇이 잘못됐는지 여전히 명확하지 않다. 여기서, ASR 5000의 제한은 Radius DM에서 Called-station-Id를 지원하지 않는다. 따라서 표시되는 경우 강조 표시된 오류와 함께 응답합니다.

<#root>

```
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)

시스템에서 "radius change-authorize-nas-ip" 줄에 "no-nas-identification-check"를 구성했습니다. "NAS-Identification-Mismatch" 오류가 계속 반환되었습니다.

이 컨피그레이션에서는 다음과 같은 작업이 수행됩니다.

```
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
+A24x0pj4mjgnqh0sc1bnen1lm6f1d6drn2nw3yf31tmf1dk9fr38e      port 1813
#exit
```

활성 PDP 컨텍스트의 경우 연결 끊기 요청이 NAKed입니다.

<#root>

```
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
```


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

또는 AAA 그룹에서 nas-식별자를 구성하지 않고 Disconnect-Request에서 NAS-Identifier AVP를 제거한 경우에도 작동합니다.

<#root>

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 버그 ID [CSCuw78786](#)이 전송되었습니다. 이 테스트는 Release 17.2.0 및 Release 15에서 수행되었습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.