Поймите и устраните неполадки RADIUS CoA и разъедините сообщения

Содержание

Введение
Определение сообщений RADIUS CoA
DM RADIUS
Атрибуты для идентификации сеанса
Конфигурация DM RADIUS
Пример конфигурации
Примеры сценария отказов
Никакие сообщения DM, полученные на стороне ASR 5000
Порт UDP 3379 имеет готовый сокет без сообщений DM
Учет запроса
Запрос отключения
Все соответствие атрибутов, но ASR 5000 передает NAK DM с сообщением об ошибках: 401 - неподдерживаемый атрибут
Система Настроила "no-nas-identification-check" в "радиусе change-authorize-nas-ip" Линия, Ошибка "Идентификационного Несоответствия NAS" Все еще Возвратилась

Введение

Этот документ описывает сообщения Разъединения с RADIUS (DM).

Определение сообщений RADIUS CoA

Сообщение изменения авторизации (CoA) используется для изменения атрибутов и фильтров данных, привязанных к пользовательскому сеансу. Поддержки системы CoA обмениваются сообщениями от аутентификации, авторизации и учета (AAA) для изменения фильтров данных, привязанных к сеансу абонента.

> **Примечание:** Фильтры в атрибутах идентификатора фильтра (если подарок в запросе) должны быть настроены в ASR 5000 для приложения к трафику пользователя. Это - форма Списков контроля доступа (ACL) и настроено в ASR 5000 с **командами ip access-list**.

Сообщение запроса CoA должно содержать атрибуты для определения пользовательского сеанса; атрибуты и фильтры данных должны быть применены к пользовательскому сеансу. Атрибут идентификатора фильтра (идентификатор атрибута 11) содержит названия

фильтров. Если ASR 5000 успешно выполняет запрос CoA, CoA ACK передают обратно в сервер RADIUS и новые атрибуты, и фильтры данных применены к пользовательскому сеансу. В противном случае CoA NAK передается с надлежащей причиной как атрибут errorcode, не внося изменений в пользовательский сеанс.

DM RADIUS

Сообщение DM используется для разъединения пользовательских сеансов в ASR 5000 от сервера RADIUS. Сообщение запроса DM должно содержать необходимые атрибуты для определения пользовательского сеанса. Если система успешно разъединяет пользовательский сеанс, ACK DM передают обратно в сервер RADIUS. В противном случае NAK DM передается с надлежащими причинами ошибки.

Как упомянуто ранее, возможно, что NAS не может соблюдать сообщения Запроса отключения или CoA-запроса по некоторым причинам. Атрибут Причины ошибки предоставляет больше подробности о причине проблемы. Это может быть включено в Disconnect-ACK, NAK Разъединения и сообщениях CoA-NAK.

Поле значения является четырьмя октетами, который содержит целое число, которое задает причину ошибки.

- Оценивает 0-199, и 300-399 зарезервированы.
- Значения 200-299 представляют успешное завершение, так, чтобы эти значения могли бы только быть переданы в Disconnect-ACK или COA-СООБЩЕНИИ-ACK и не ДОЛЖНЫ быть переданы в NAK Разъединения или CoA-NAK.
- Значения 400-499 представляют фатальные ошибки, совершенные сервером RADIUS, так, чтобы они могли быть переданы в рамках сообщений CoA-NAK или NAK Разъединения и НЕ ДОЛЖНЫ были быть переданы в рамках сообщений CoA-ACK или Disconnect-ACK.
- Значения 500-599 представляют фатальные ошибки, которые происходят на NAS или RADIUS прокси, так, чтобы они могли быть переданы в рамках сообщений CoA-NAK и NAK Разъединения и НЕ ДОЛЖНЫ были быть переданы в рамках сообщений CoA-ACK или Disconnect-ACK. Причина ошибки оценивает SHOULD быть зарегистрированной сервером RADIUS.

Значения errorcode (выраженный в десятичном числе) включают:

```
#    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
```

Атрибуты для идентификации сеанса

Для идентификации ASR 5000 может использоваться один из этих методов:

- Nas-ip-address: IP-адрес NAS, если подарок в запросе COA/DM должен совпасть с IP-адресом ASR 5000 NAS.
- Идентификатор NAS: Если этот атрибут присутствует, его значение должно совпасть к nas-идентификатору, генерируемому для пользовательского сеанса.
  Если ASR 5000 настроен с Идентификатором NAS, это - Обязательный атрибут для идентификации сеанса.

Для идентификации пользовательского сеанса используется любой из этих методов:

- Acct-идентификатор-сеанса: Если этот атрибут присутствует, его значение должно совпасть к acct-идентификатору-сеанса для пользовательского сеанса.
- ОБРАМЛЕННЫЙ IP-АДРЕС: Если этот атрибут присутствует, его значения должны совпасть к обрамленному IP-адресу сеанса.
- Username: Если этот атрибут присутствует, его значения должны совпасть к имени пользователя сеанса.
- Calling-Station-ID: Это - Международный идентификатор мобильного абонента (IMSI) пользователя.

Конфигурация DM RADIUS

Конфигурация DM RADIUS довольно легка. Все линии должны быть настроены в целевом контексте (тот с Конфигурацией RADIUS).

радиус change-authorize-nas-ip *ip_address* **[зашифровал] значение параметра [***порт* **порта] [***окно* **eventtimestamp-окна] [no-nas-identification-check]**
[no-reverse-path-forward-check] [mpls label вводят *in_label_value* **| выходные данные out_label_value1**
[out_label_value2]

> **Примечание:** "Радиус change-authorize-nas-ip" должен быть адресом интерфейса AAA вашего локального контекста. Эта команда CLI иногда является источником беспорядка.

Пример конфигурации

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

Примеры сценария отказов

Никакие сообщения DM, полученные на стороне ASR 5000

Возможно, что сокет не готов к порту 3799 UDP. (В соответствии с RFC 3756, пакет Запроса отключения RADIUS передан к порту 3799 UDP).

Это поведение может быть упрощено. Процесс, который обрабатывает все запросы CoA, является aaamgr экземпляром 385, который является тем на активной карте SMC/MIO. Эта команда CLI должна быть выполнена в целевом контексте.

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

Такие выходные данные похожи:

```
# 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
```

В данном примере нет никакого порта 3799, и это - причина для поведения, о котором сообщают. Если вы видите то же в своем случае, решение состоит в том, чтобы удалить и повторно добавить конфигурацию CoA для воссоздания сокета прослушивания. Если первое решение не помогает, Кроме того, можно попытаться уничтожить aaamgr экземпляр 385.

После описанных действий необходимо видеть эти выходные данные:

```
# 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
```

и сокет должен быть видим от оболочки отладки на соответствующем контексте/VR:

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

Порт UDP 3379 имеет готовый сокет без сообщений DM

Порт 3379 UDP имеет готовый сокет, однако вы все еще не видите сообщения DM. Это, вероятно, вызвано некорректной конфигурацией радиуса change-authorize-nas-ip. Любой значения атрибута, которые поступили в сообщение запроса DM, не совпадают с теми,

которые передавались в Бухгалтерском запросе к RADIUS.

Учет запроса

```
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)
```

Запрос отключения

```
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
```

В данном примере значение **Acct-идентификатора-сеанса**, который прибывает в ASR 5000, является другим, чем тот, передаваемый к RADIUS, и это - причина для проблемы. Эта проблема может быть решена надлежащими изменениями на стороне RADIUS.

Acct-идентификатор-сеанса для активного сеанса может быть проверен с командой, **показывают абонентам ggsn-только aaa configuration активный 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
```

Все соответствие атрибутов, но ASR 5000 передает NAK DM с сообщением об ошибках: 401 - неподдерживаемый атрибут

На этом этапе известно, что это сообщение типа ошибки означает, что проблема прибывает из сервера RADIUS. Однако это все еще не ясно что не так. Здесь, ограничение ASR 5000 не поддерживает Вызванный идентификатор станции в DM Радиуса. Следовательно, если это замечено там, отвечает это с выделенной ошибкой.

```
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)
```

Система Настроила "no-nas-identification-check" в "радиусе change-authorize-nas-ip" Линия, Ошибка "Идентификационного Несоответствия NAS" Все еще Возвратилась

Это происходит в этой конфигурации:

```
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
```

Для активного контекста PDP Запрос отключения является ЯВНЫМ:

```
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)
```

Однако, когда эта линия включена в группу AAA по умолчанию:

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

это начинает работать:

```
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
```

Или это будет также работать без конфигурации nas-идентификатора на группе AAA, но с AVP Идентификатора NAS, удаленным из Запроса отключения:

```
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
```

Идентификатор ошибки Cisco CSCuw78786 был отправлен. Это было протестировано на Выпуске 17.2.0 и Выпуске 15.