فهم CoA ل RADIUS واستكشاف أخطائه وإصلاحها وفصل الرسائل

المحتويات

المقدمة

يوضح هذا المستند رسائل RADIUS الخاصة بفصل (DMs).

تعريف رسائل RADIUS CoA

يتم إستخدام رسالة "تغيير التفويض (CoA)" لتغيير السمات ومرشحات البيانات المقترنة بجلسة عمل المستخدم. يدعم النظام رسائل CoA من خادم المصادقة والتفويض والمحاسبة (AAA) لتغيير عوامل تصفية البيانات المرتبطة بجلسة عمل المشترك.

ملاحظة: يجب تكوين عوامل التصفية في سمات معرف التصفية (إن كانت موجودة في الطلب) في ASR 5000 للتطبيق على حركة مرور المستخدم. هذا هو شكل قوائم التحكم في الوصول (ACL) وتم تكوينها في ASR 5000 باستخدام أوامر **ip access-list**.

يجب أن تحتوي رسالة طلب CoA على سمات لتعريف جلسة عمل المستخدم؛ يجب تطبيق السمات وعوامل تصفية البيانات على جلسة عمل المستخدم. تحتوي سمة معرف عامل التصفية (معرف السمة 11) على أسماء عوامل التصفية. إذا قام ASR 5000 بتنفيذ طلب CoA بنجاح، يتم إرسال ACK مرة أخرى إلى خادم RADIUS ويتم تطبيق مرشحات السمات والبيانات الجديدة على جلسة عمل المستخدم. وإلا، يتم إرسال NAK مع سبب مناسب كسمة رمز خطأ دون إجراء أي تغييرات على جلسة عمل المستخدم.

RADIUS DM

يتم إستخدام رسالة DM لقطع اتصال جلسات عمل المستخدم في ASR 5000 من خادم RADIUS. يجب أن تحتوي رسالة طلب إدارة قاعدة البيانات على السمات الضرورية لتحديد جلسة عمل المستخدم. في حالة قطع النظام لجلسة عمل المستخدم بنجاح، يتم إرسال ACK إلى خادم RADIUS. وإلا، يتم إرسال DM-NAK لأسباب خطأ صحيحة.

وكما تمت الإشارة مسبقا، قد لا يتمكن NAS من إحترام رسائل Disconnect-Request أو CoA-Request لسبب ما. توفر سمة سبب الخطأ المزيد من التفاصيل حول سبب المشكلة. يمكن تضمينها ضمن رسائل Disconnect-ACK و Disconnect-NAK و CoA-NAK.

حقل القيمة هو أربع أنظمة ثمانية، تحتوي على عدد صحيح يحدد سبب الخطأ.

- القيم **0-199** و**300-399** محجوزة.
- تمثل القيم **200-299** إكمال ناجح، لذلك قد يتم إرسال هذه القيم فقط ضمن رسالة Disconnect-ACK أو CoA-ACK ويجب عدم إرسالها ضمن Disconnect-NAK أو CoA-NAK.
- تمثل القيم **400-499** أخطاء فادحة ارتكبها خادم RADIUS، حتى يمكن إرسالها ضمن رسائل CoA-NAK أو قطع اتصال-NAK ويجب عدم إرسالها ضمن رسائل CoA-ACK أو قطع اتصال ACK.
- تمثل القيم **500-599** أخطاء قاتلة تحدث على وكيل NAS أو RADIUS، لذلك يمكن إرسالها ضمن رسائل -CoA NAK و Disconnect-NAK، ويجب عدم إرسالها ضمن رسائل CoA-ACK أو Disconnect-ACK. يجب تسجيل قيم سبب الخطأ بواسطة خادم RADIUS.

تتضمن قيم رمز الخطأ (معبرا عنها بالعشري):

#	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

سمات تعريف الجلسة

لتعريف ASR 5000، يمكن إستخدام إحدى الطريقتين التاليتين:

- عنوان NAS-IP: يجب أن يتطابق عنوان IP ل NAS إن كان موجودا في طلب COA/DM مع عنوان IP ل ASR 5000 NAS.
- معرف NAS: إذا كانت هذه السمة موجودة، فيجب أن تتطابق قيمتها مع معرف NAS الذي تم إنشاؤه لجلسة عمل المستخدم.
  هذه سمة إلزامية لتعريف جلسة العمل، إذا تم تكوين ASR 5000 باستخدام معرف NAS.

لتعريف جلسة عمل المستخدم، يتم إستخدام أحد الطريقتين التاليتين:

- Acct-Session-ID: إذا كانت هذه السمة موجودة، يجب أن تتطابق قيمتها مع Access-session-id لجلسة عمل المستخدم.
- Framed-IP-Address: إذا كانت هذه السمة موجودة، يجب أن تتطابق قيمها مع عنوان IP المؤطر للجلسة.
- اسم المستخدم: إذا كانت هذه السمة موجودة، فيجب أن تتطابق قيمها مع اسم المستخدم للجلسة.
- Call-Station-ID: هذه هي هوية مشترك الهاتف المحمول الدولية (IMSI) للمستخدم.

تكوين RADIUS DMs

تكوين RADIUS DM سهل للغاية. يجب تكوين جميع الخطوط في سياق الوجهة (الخط ذو تكوين RADIUS).

RADIUS change-authorize-NAS-IP *ip_address* **مفتاح [المشفر]** *القيمة* **[المنفذ** *المنفذ* **]**
[eventTimestamp-window *نافذة* **] [التحقق من عدم وجود أسماء لتحديد الهوية]**
[لا-عكسي-مسار-للأمام][*in_label_value* **MPLS-Label input | الناتج** *out_label_value1*
[*out_label_value2* **]**

ملاحظة: يجب أن يكون "RADIUS change-authorize-nas-ip" عنوان واجهة AAA للسياق المحلي لديك.
إن أمر واجهة سطر الأوامر (CLI) هذا يكون في بعض الأحيان مصدر إرتباك.

عينة من التكوين

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

أمثلة سيناريو الفشل

لم يتم تلقي رسائل DM على جانب ASR 5000

من المحتمل أن يكون المأخذ غير جاهز لمنفذ UDP 3799. (وفقا ل RFC 3756، يتم إرسال حزمة طلب قطع اتصال RADIUS إلى منفذ UDP 3799).

يمكن تبسيط هذا السلوك. العملية التي تتعامل مع جميع طلبات CoA هي مثيل 385، وهو المثيل الموجود على بطاقة SMC/MIO النشطة. يجب تنفيذ أمر واجهة سطر الأوامر (CLI) هذا في سياق الوجهة.

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

ويبدو مثل هذا المخرج:

```
: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
```

في هذا المثال، لا يوجد منفذ 3799 وهذا هو سبب السلوك الذي تم الإبلاغ عنه. إذا رأيت نفس الشيء في حالتك، فإن الحل هو إزالة تكوين CoA وإعادة إضافته لإعادة إنشاء مأخذ الاستماع. بالإضافة إلى ذلك، يمكنك محاولة القضاء على مثيل 385 في حالة أن الحل الأول لا يساعد.

بعد العمليات الموصوفة، يجب أن ترى هذا المخرج:

```
: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
```

ويجب أن يكون المقبس مرئيا من صدفة تصحيح الأخطاء على السياق/VR المناسب:

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

منفذ UDP رقم 3379 مزود بمقبس جاهز بدون رسائل DM

يكون منفذ UDP 3379 جاهزا للمأخذ، ومع ذلك ما زلت لا ترى رسائل DM. قد يكون هذا بسبب تكوين غير صحيح ل **RADIUS change-authorize-nas-ip**. إما أن قيم السمات التي جاءت في رسالة طلب DM لا تتطابق مع القيم التي تم إرسالها في طلب محاسبة باتجاه RADIUS.

طلب المحاسبة

```
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
0603A2BF 46 42 32 41 33 30 36 30
(Attribute Type: 31 (Calling-Station-Id
Length: 14
Value: 39 39 38 39 33 31 37 32 99893172
0911            31 31 39 30
(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)
```

طلب قطع الاتصال

```
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
```

في هذا المثال، تختلف قيمة **Acct-Session-ID** التي تأتي إلى ASR 5000 عن تلك التي يتم إرسالها نحو RADIUS وهذا هو سبب المشكلة. يمكن إصلاح هذه المشكلة من خلال التغييرات المناسبة في جانب RADIUS.

يمكن التحقق من معرف Acct-Session للجلسة النشطة باستخدام الأمر **show subscribers-only aaa-configuration active 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
```

تتطابق كافة السمات، ولكن ASR 5000 يرسل DM NAK مع رسالة الخطأ: 401 - سمة غير مدعومة

عند هذه النقطة من المعروف أن هذا النوع من رسائل الخطأ يعني أن المشكلة تأتي من خادم RADIUS. بيد انه لم يتضح بعد ما هو الخطأ. هنا، لا يدعم تحديد ASR 5000 معرف المحطة الاستدعاء في RADIUS DM. لذلك، إذا كان يرى هناك، يجيب بالخطأ المبرز.

```
<<<<<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
                                      567              37 36 35

                                (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)
```

قام النظام بتكوين "no-nas-identification-check" في السطر "radius change-authorize-nas-ip"، وما زال الخطأ "NAS-IDENTIFICATION-MISMATCH" مرتجعا

يحدث هذا في هذا التكوين:

```
                                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#
```

بالنسبة لسياق PDP نشط، يكون طلب قطع الاتصال هو 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-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
nbsp                Value: 36 34 32 31 31 32 33 34 64211234;     Length: 13&

                                      567              37 36 35
```

```
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)
```

ومع ذلك، عند تضمين هذا السطر في مجموعة AAA الافتراضية:

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

بيبلش يشتغل:

```
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
```

أو سيعمل أيضا دون تكوين معرف NAS على مجموعة AAA، ولكن مع إزالة AVP لمعرف NAS من طلب قطع الاتصال:

```
(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
```

تم إرسال معرف تصحيح الأخطاء من Cisco CSCuw78786. وقد تم إختبار ذلك في الإصدار 17.2.0 والإصدار 15.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).