

知 某局点通过Radius DM消息报文下发离线失败问题

Portal AAA 朱楷 2023-04-18 发表

组网及说明

产品： WX3540X （用新款V9 AC替换之前的V5 AC）

现象： portal认证，radius服务器踢用户需要通过DAE下发DM消息给AC，在V5环境可以稳定可用，但是在V9 AC环境下发现无法踢用户。

问题描述

现象：portal认证，radius服务器踢用户需要通过DAE下发DM消息给AC，在V5环境可以稳定可用，但是在V9 AC环境下发现无法踢用户。

过程分析

对交互的radius报文进行抓包分析。按照acct-session-id进行检索区分

先看V5正常的报文内容：

1、V5环境的历史在线报文。

显示Acct-session-id为 1230414105228160fa68262ef5

Calling-station-id为12-20-BD-2C-79-A3

Framed-IP-Address为10.216.143.69

No.	Time	Source	Destination	Protocol	Length	Acct-Session-Id	Info
1	2023-04-14 10:51:36.94.	172.16.95.23	172.16.95.23	RADIUS	110	1230414105228160fa68262ef5	Disconnect-Request id=3
2	2023-04-14 10:51:36.94.	172.16.95.23	172.16.95.23	RADIUS	122	1230414105228160fa68262ef5	Disconnect-ACK id=35
3	2023-04-14 10:51:37.56.	172.16.95.23	172.16.95.23	RADIUS	413	1230414105228160fa68262ef5	Accounting-Request id=4

```
> AVP: t:NAS-Port-Type(61) l=6 val=Wireless-802.11(18)
> AVP: t:Calling-Station-Id(31) l=19 val=12-20-BD-2C-79-A3
> AVP: t:Called-Station-Id(30) l=33 val=
> AVP: t:Acct-Status-Type(40) l=6 val=Stop(2)
> AVP: t:Acct-Authenticate(45) l=6 val=RADIUS(1)
> AVP: t:Acct-Session-Id(44) l=28 val=1230414105228160fa68262ef5
> AVP: t:Framed-IP-Address(8) l=6 val=10.216.143.69
> AVP: t:NAS-IP-Address(4) l=6 val=
> AVP: t:Event-Timestamp(55) l=6 val=Apr 14, 2023 10:53:32.000000000 中国标准时间
> AVP: t:Filter-Id(11) l=6 val=3111
> AVP: t:Acct-Session-Time(46) l=6 val=64
> AVP: t:Acct-Delay-Time(41) l=6 val=0
> AVP: t:Acct-Input-Octets(42) l=6 val=61655
> AVP: t:Acct-Input-Packets(47) l=6 val=174
> AVP: t:Acct-Output-Octets(43) l=6 val=60314
> AVP: t:Acct-Output-Packets(48) l=6 val=160
> AVP: t:Acct-Input-Gigawords(52) l=6 val=0
> AVP: t:Acct-Output-Gigawords(53) l=6 val=0
> AVP: t:Acct-Terminate-Cause(49) l=6 val=Admin-Reset(6)
```

2、V5环境下AAA下发的DM请求消息内容

显示Acct-session-id为 1230414105228160fa68262ef5

Calling-station-id为1220BD2C79A3 //与AC记录的12-20-BD-2C-79-A3格式不太一样

Framed-IP-Address为10.216.143.69

No.	Time	Source	Destination	Protocol	Length	Acct-Session-Id	Info
1	2023-04-14 10:51:36.94.	172.16.95.23	172.16.95.23	RADIUS	110	1230414105228160fa68262ef5	Disconnect-Request id=3
2	2023-04-14 10:51:36.94.	172.16.95.23	172.16.95.23	RADIUS	122	1230414105228160fa68262ef5	Disconnect-ACK id=35
3	2023-04-14 10:51:37.56.	172.16.95.23	172.16.95.23	RADIUS	413	1230414105228160fa68262ef5	Accounting-Request id=4

```
> Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
> Ethernet II, Src: 9c:69:b4:60:48:8c, Dst: 00:09:0f:09:0e:1c
> Internet Protocol Version 4, Src: 172.16.95.23, Dst: 172.16.95.23
> User Datagram Protocol, Src Port: radius (1812), Dst Port: radius-aynauth (3799)
RADIUS Protocol
Code: Disconnect-Request (40)
Packet identifier: 0x23 (35)
Length: 68
Authenticator: a640b9a01f8738ad41f99c95510785c
Attribute Value Pairs
> AVP: t:Framed-IP-Address(8) l=6 val=10.216.143.69
> AVP: t:Calling-Station-Id(31) l=14 val=1220BD2C79A3
> AVP: t:Acct-Session-Id(44) l=28 val=1230414105228160fa68262ef5
```

3、V5环境下AC下发的DM ACK内容

No.	Time	Source	Destination	Protocol	Length	Acct-Session-Id	Info
1	2023-04-14 10:51:36.94.	172.16.95.23	172.16.95.23	RADIUS	110	1230414105228160fa68262ef5	Disconnect-Request id=3
2	2023-04-14 10:51:36.94.	172.16.95.23	172.16.95.23	RADIUS	122	1230414105228160fa68262ef5	Disconnect-ACK id=35
3	2023-04-14 10:51:37.56.	172.16.95.23	172.16.95.23	RADIUS	413	1230414105228160fa68262ef5	Accounting-Request id=4

```
> Frame 2: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
> Ethernet II, Src: 00:09:0f:09:0e:1c, Dst: 9c:69:b4:60:48:8c
> Internet Protocol Version 4, Src: 172.16.95.23, Dst: 172.16.95.23
> User Datagram Protocol, Src Port: radius-aynauth (3799), Dst Port: radius (1812)
RADIUS Protocol
Code: Disconnect-ACK (41)
Packet identifier: 0x23 (35)
Length: 80
Authenticator: 2afdc23f98c4f454acc6ca86c4fa3666
[This is a response to a request in frame 1]
[Time from request: 0.001945000 seconds]
Attribute Value Pairs
> AVP: t:Acct-Session-Id(44) l=28 val=1230414105228160fa68262ef5
> AVP: t:Framed-IP-Address(8) l=6 val=10.216.143.69
> AVP: t:Calling-Station-Id(31) l=14 val=1220BD2C79A3
> AVP: t:Error-Cause(101) l=6 val=Residual-Context-Removed(201)
> AVP: t:Acct-Terminate-Cause(49) l=6 val=Admin-Reset(6)
```

再看V9异常的报文内容：

1、V9环境的历史在线报文。

显示Acct-session-id为 0000000704170302350000004a08000001320

Calling-station-id为B2-80-BB-7C-4C-D2

Framed-IP-Address为10.213.220.15

上述抓包分析，虽然服务器下发了格式一样的DM请求报文，但是AC设备的匹配策略不同。实际调查发现，V5平台的处理策略是在DAE DM消息检查时是宽松的匹配方式。只要Acct-Session-ID能匹配就认为能找到会话。其他消息字段不填或者填错都不会影响判断结果。

而对应的V9平台的处理策略是严格匹，默认V9需要携带的所有信息都要匹配上报文才能继续处理。也就是说不光Acct-Session-ID一样匹配，就连其他的属性字段也要一模一样匹配，否则就会认为消息字不符合。因此V9开启了严格的匹配策略，只要acct-session-id符合就可以。

radius.dynamic-authentication-server clientip X:X:X:key-cipher-0x33ullSkpHFBGuo1GPXdDp/C33kJFVImLhuNA==
dae-check-enable //开启DAE报文的宽松检查功能 只会校验DAE报文中的部分用户标识信息 (用户IP地址、Acct-Session-Id以及纯用户名部分)，不再校验设备标识信息。

2、V9环境AAA下发的DM请求消息。

显示Acct-session-id为 00000070417030235000004a0800001320

Calling-station-id为B280BB7C4CD2 //格式风格不一样 没有携带“-”字符

Framed-IP-Address为10.213.220.15

Frame 28013: 121 bytes on wire (968 bits), 121 bytes captured (968 bits) on interface
 Ethernet II, Src: 9c:69:b4:60:48:8c, Dst: 00:09:0f:09:0e:1c
 Internet Protocol Version 4, Src: 172.16.95.23, Dst: 172.16.95.23
 User Datagram Protocol, Src Port: radius (1812), Dst Port: radius-dynauth (3799)
 RADIUS Protocol
 Code: Disconnect-Request (40)
 Packet Identifier: 0x2e (46)
 Length: 79
 Authenticator: 45297e679b272761c3f2e48a0e6a9d5f
 [This response to this request is in frame 28014]
 Attribute Value Pairs
 AVP: tFramed-IP-Address(8) l=6 val=10.213.220.15
 AVP: tCalling-Station-Id(31) l=14 val=B280BB7C4CD2
 AVP: tAcct-Session-Id(44) l=39 val=00000070417030235000004a0800001320

3、V9环境AC回应的DM NAK消息。

显示没法发现这个会话信息

Frame 28014: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface
 Ethernet II, Src: 00:09:0f:09:0e:1c, Dst: 9c:69:b4:60:48:8c
 Internet Protocol Version 4, Src: 172.16.95.23, Dst: 172.16.95.23
 User Datagram Protocol, Src Port: radius-dynauth (3799), Dst Port: radius (1812)
 RADIUS Protocol
 Code: Disconnect-NAK (42)
 Packet Identifier: 0x2e (46)
 Length: 72
 Authenticator: 450857205a07773d0e864ccdf5ea23
 [This is a response to a request in frame 28013]
 [Time from request: 0.000970000 seconds]
 Attribute Value Pairs
 AVP: tFramed-IP-Address(8) l=6 val=10.213.220.15
 AVP: tAcct-Session-Id(44) l=40 val=00000070417030235000004a0800001320000
 AVP: tError-Cause(181) l=6 val=Session-Context-Not-Found(503)

