

某局点使用iNode结合锐捷交换机（等第三方）802.1x认证提示用户不存在的原因分析

寻岩岩 2017-08-14 发表

现场使用iNode结合锐捷交换机做802.1x认证，终端使用静态IP地址，勾选了上传客户端版本号和IP地址两个选项，服务器使用EIA。用户认证时提示用户名为空或者用户不存在或者没有申请该服务。

用户认证时提示用户不存在或者没有申请该服务。

分析服务器UAM调试日志，发现Radius报文里面User-Name为空，如下图所示，所以用户认证时会提示用户不存在。

CODE = 1.

ID = 109.

ATTRIBUTES:

User-Name(1) = "..."

Service-Type(6) = 2.

Framed-MTU(12) = 1500.

EAP-Message(79) =

"0200202904107a641759202816286f66b03f37153b237a68616e676a696e6775616e5f776c406f7072".

Message-Authenticator(80) = "9fd0dd61cc66689a282c6329429921e6".

Attribute (0-102) is not defined in dic file r2.

NAS-Port-Type(61) = 15.

继续分析服务器抓包，发现接入设备传过来的user-name里面是有值的，具体值为：15 04 16 1a 00 a8 06.....，UAM发现该字节流里面有00.00在编程语言表示结束的意思，所以UAM会截取15 04 16 1a为用户名，而15 04 16 1a为不可见字符，所以最终UAM提示用户名为空。

18941	2017-07-17 16:00:55.149945	22.26.0.190	22.24.1.196	RADIUS	320 Access-Request(1) (id=169, l=278)
18943	2017-07-17 16:00:55.150369	22.24.1.196	22.26.0.190	RADIUS	158 Access-Reject(3) (id=169, l=116)
29657	2017-07-17 16:01:05.606057	22.26.0.190	22.24.1.196	RADIUS	320 Access-Request(1) (id=170, l=278)
29658	2017-07-17 16:01:05.606561	22.24.1.196	22.26.0.190	RADIUS	158 Access-Reject(3) (id=170, l=116)
38009	2017-07-17 16:01:15.885959	22.26.0.190	22.24.1.196	RADIUS	320 Access-Request(1) (id=171, l=278)
38100	2017-07-17 16:01:15.886385	22.24.1.196	22.26.0.190	RADIUS	158 Access-Reject(3) (id=171, l=116)
45718	2017-07-17 16:01:26.080781	22.26.0.190	22.24.1.196	RADIUS	320 Access-Request(1) (id=172, l=278)
45719	2017-07-17 16:01:26.081253	22.24.1.196	22.26.0.190	RADIUS	158 Access-Reject(3) (id=172, l=116)

Frame 18941: 320 bytes on wire (2560 bits), 320 bytes captured (2560 bits)
Ethernet II, Src: Hangzhou_2e:61:f0 (c4:ca:d9:2e:61:f0), Dst: 1bm_48:02:4a (08:be:94:48:02:4a)
Internet Protocol Version 4, Src: 22.26.0.190, Dst: 22.24.1.196
User Datagram Protocol, Src Port: 39559 (39559), Dst Port: 1812 (1812)
RADIUS Protocol
Code: Access-Request (1)
Packet Identifier: 0xa9 (169)
Length: 278
Authenticator: dffdf02fed02b70c6a2563ba49e22cc
[The response to this request is in frame 18943]
Attribute Value Pairs
User-Name(1): 025\004\026\032\000\250\006\1a02g3Gh8PCB5R8tklIfxYwSwI= test123111
NAS-Port-Type(61): 15
AVP: 1-6 t=NAS-Port-Type(61): Ethernet(15)

050	15 04 16 1a 00 a8 06 07 4f 32 67 4a 47 68 38 4a	----- User-Name
050	50 41 42 35 52 42 74 60 49 6c 46 76 4b 50 77 53	----- User-Name
060	5c 46 78 4b 50 77 53 77 76 40 3d 20 20 74 65 76	----- User-Name
070	57 16 47 69 67 61 62 69 74 45 74 68 65 72 6e 65	----- User-Name
080	74 20 30 2f 33 38 3d 06 00 00 0f 08 06 00 00	----- User-Name

现场接入设备是第三方设备，配置的EAP模式，EAP模式下设备仅仅透传客户端的认证报文，所以该字节流应该是客户端传过来的。

分析客户端侧抓包，发现客户端封装的EAP报文的identity字段就是以15 04开头的，所以可以明确原始报文是iNode生成的。iNode在填充identity字段时为何不直接填充用户名而是要以15 04开头呢，这是因为为了实现我司的一些私有功能而设置的特殊标识，目的就是告诉交换机后面紧跟的一些字节是iNode上传的一些用户属性。比如以15 04开头时就表示后面紧跟的4字节是用户IP地址；以06 07开头时表示后面紧跟的30字节是客户端版本号，设备发现以1504开头或者0607开头就知道后面紧跟的是IP地址和客户端版本号了，同时交换机会提取出相关属性后重新封装到Radius报文转给UAM，而现场的第三方交换机不识别该标识，所以把EAP报文整体传给了UAM，最终导致出问题。

> Frame 11: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
> Ethernet II, Src: d4:81:d7:33:c6:25 (d4:81:d7:33:c6:25), Dst: Nearest (01:80:c2:00:00:03)
802.1X Authentication
Version: 802.1X-2001 (1)
Type: EAP Packet (0)
Length: 53
Extensible Authentication Protocol
Code: Response (2)
Id: 1
Length: 53
Type: Identity (1)
Identity: \025\004\026\032

0000	01 80 c2 00 00 03 d4 81 d7 33 c6 25 88 8e 01 00	3..
0010	00 35 02 01 00 35 01 15 04 16 1a 00 a8 06 07 4f	..5...S.....
0020	52 67 4a 47 68 38 4a 50 43 42 35 52 42 74 60 49	g3Gh8PCB5R8tkl
0030	5c 46 78 4b 50 77 53 77 76 40 3d 20 20 74 65 76	lIfxYwSw vi= te
0040	74 31 32 33 31 31 31	123111

为了进一步确认问题，再看iNode封装的报文顺序，发现data部分是按照IP地址、客户端版本号、账号名的顺序封装的。IP地址以15 04开头，后面的16 1a 00 a8就是22.26.0.168.再往后是0607,0607后面的4开头的就是客户端版本号。

Code (1): Response ---- 02

Id (1): 1 ---- 01

Length (2): 53 ---- 00 35

Data Type (1): ID ---- 01

IPv4 (4): 22.26.0.168

CliVer (30):

4f 32 67 4a 47 68 38 44 50 43 42 35 52 42 74 6b

49 6c 46 78 4b 59 77 53 77 76 49 3d 20 20

O2gJGh8DPCB5RBtklIFxKYwSwvl=

Username (10):

74 65 73 74 31 32 33 31 31 31

test123111

iNode去勾选“上传IP地址”;

更换我司交换机;

终端侧IP地址不要包含0段。

以上三选一即可

1504后面的4个字节标识ip地址; 0607 (0608是针对域账号) 后面的30个字节是客户端版本号。