

知 某局点iNode结合EIA 802.1x认证失败的典型案例

iMC UAM 马永鸿 2023-03-31 发表

组网及说明

无

告警信息

无

问题描述

客户现场用iNode配合iMC EIA做802.1x认证，接入设备是第三方交换机。测试时认证失败，查看认证失败日志，失败原因为“E63018：用户不存在或者用户没有申请该服务”。且登录名存在乱码。

用户 > 用户接入日志 > 认证失败日志

认证失败日志查询

认证失败日志列表

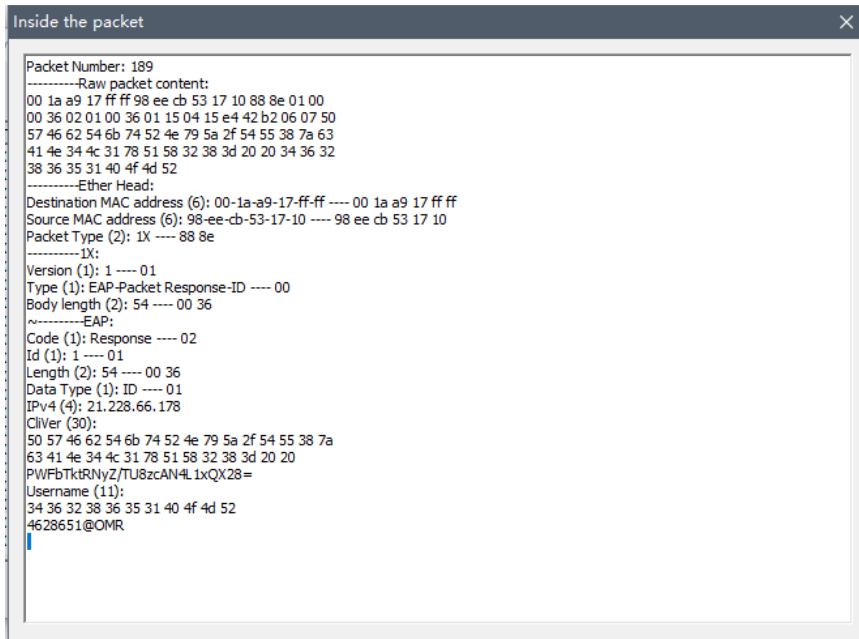
批量导出 清除认证失败原因

帐号名	登录名	服务名称	认证失败原因	认证失败时间
%? OGhaHhtQPIN6RE5jAjKuQ2yHU= 4628651@omr	%? bDNZFxlTZXCouH01qKQEqWZivF0= 4628651@omr		E63018: 用户不存在或者用户没有申请该服务。	2023-03-06 18:11:49
%? MmMPFBEFNShwTxdpKd8IEx6okE= 4628651@omr	%? N2BZEBVTNo1TE1tLgFSJclPuJw= 4628651@omr		E63018: 用户不存在或者用户没有申请该服务。	2023-03-06 18:10:29
%? bWcGT0cMMXyYsdyCV5-f770Sw= 4628651@omr	%? aGRZT0pTMmMqSE0ycQF9ej3xNyc= 4628651@omr		E63018: 用户不存在或者用户没有申请该服务。	2023-03-06 18:09:50
%? OGhaHhtQPIN6RE5jAjKuQ2yHU= 4628651@omr			E63018: 用户不存在或者用户没有申请该服务。	2023-03-06 18:08:53
%? OGhaHhtQPIN6RE5jAjKuQ2yHU= 4628651@omr			E63018: 用户不存在或者用户没有申请该服务。	2023-03-06 18:07:05
%? OGhaHhtQPIN6RE5jAjKuQ2yHU= 4628651@omr			E63018: 用户不存在或者用户没有申请该服务。	2023-03-06 18:05:46

共有6条记录, 当前第1-6, 第 1/1 页。

过程分析

1. 首先排查EIA配置方面，已确认该用户名存在，且已绑定接入服务，服务后缀和域名的关系也都符合。配置方面没发现问题。
2. 收集iNode 详细级别日志，分析EAP报文交互情况。



```
Inside the packet
Packet Number: 189
-----Raw packet content:
00 1a a9 17 ff ff 98 ee cb 53 17 10 88 8e 01 00
00 36 02 01 00 36 01 15 04 15 e4 42 b2 06 07 50
57 46 62 54 6b 74 52 4e 79 5a 2f 54 55 38 7a 63
41 4e 34 4c 31 78 51 58 32 38 3d 20 20 34 36 32
38 36 35 31 40 4f 4d 52
-----Ether Head:
Destination MAC address (6): 00-1a-a9-17-ff-ff ---- 00 1a a9 17 ff ff
Source MAC address (6): 98-ee-cb-53-17-10 ---- 98 ee cb 53 17 10
Packet Type (2): 1X ---- 88 8e
-----1X:
Version (1): 1 ---- 01
Type (1): EAP-Packet Response-ID ---- 00
Body length (2): 54 ---- 00 36
-----EAP:
Code (1): Response ---- 02
Id (1): 1 ---- 01
Length (2): 54 ---- 00 36
Data Type (1): ID ---- 01
IPv4 (4): 21.228.66.178
ClVer (30):
50 57 46 62 54 6b 74 52 4e 79 5a 2f 54 55 38 7a
63 41 4e 34 4c 31 78 51 58 32 38 3d 20 20
PWFBtkrNyZ/TU8zcAN4L1xQX28=
Username (11):
34 36 32 38 36 35 31 40 4f 4d 52
4628651@OMR
```

在EAP-Response报文中，可以看到Username这一字段，用户名4628651@OMR前面确实多出了一串字符。

经确认，问题原因是iNode客户端在802.1x连接属性中勾选了“上传客户端版本号”，在用户名前多出的那一串字符就是客户端版本号。对于我司设备，正常情况都可以解析出用户名；而对于友商设备，则无法从Username这一字段正确解析出用户名和客户端版本号了，因此将整个字段的字符串当成用户名，从而认证失败

解决方法

如果接入设备是第三方设备，在用iNode做802.1x认证时，不勾选“上传客户端版本号”。

802.1X认证

常规 网络 高级

连接名 802.1X连接

选择网卡
Npcap Loopback Adapter:Npcap Loopback Ad...

连接类型

<input checked="" type="radio"/> 普通连接	<input type="radio"/> 入网认证
<input type="radio"/> 快速认证连接	<input type="radio"/> 补充认证
<input type="radio"/> 单点登录连接	<input type="radio"/> 全网认证

运行后自动认证

计算机认证

上传客户端版本号

认证时清除ARP表项

有线环境下自动认证

确定 取消

