

# 知 华三设备对接第三方Free radius认证服务器将我司设备识别为华为设备从而获取到错误的权限解决方法

Radius AAA zhiliao\_fE11i8 2024-05-15 发表

## 组网及说明

Free-radius 版本: FreeRADIUS Version 3.0.13  
操作系统: Oracle Linux Server 7.8  
我司交换机型号: S5170-28S-HPWR-EI  
我司交换机版本: Version 7.1.070, Release 1115

## 告警信息

我司设备接口上线触发AAA认证获取到的是华为设备的权限

```
*Mar 27 13:06:16:294 2024 H3C_PRUEBAS RADIUS/7/PACKET:
Service-Type=NAS-Prompt-User
Service-Type=Administrative-User
Vendor-2636-Attr-1=0x6f70657261646f72
Hw-Exec-Privilege=3
Vendor-12356-Attr-1=0x4669726577616c6c5f41646d696e73
Vendor-5003-Attr-35=0x000000c8
Vendor-28557-Attr-2=0x0000001f
Vendor-28557-Attr-1=0x00000000
Vendor-28557-Attr-4=0x0000003f
Vendor-28557-Attr-3=0xffffffff
Cisco-AVPair="shell:priv-lvl=15"
Vendor-3224-Attr-1=0x00000001
*Mar 27 13:06:16:295 2024 H3C_PRUEBAS RADIUS/7/PACKET:
02 ba 00 b4 7f 55 52 7e 97 73 e4 81 2b 9a a5 32
1a b0 ec 23 06 06 00 00 00 07 06 06 00 00 00 06
1a 10 00 00 0a 4c 01 0a 6f 70 65 72 61 64 6f 72
1a 0c 00 00 07 db 1d 06 00 00 00 03 1a 17 00 00
30 44 01 11 46 69 72 65 77 61 6c 6c 5f 41 64 6d
69 6e 73 1a 0c 00 00 13 8b 23 06 00 00 00 c8 1a
0c 00 00 6f 8d 02 06 00 00 00 1f 1a 0c 00 00 6f
8d 01 06 00 00 00 00 1a 0c 00 00 6f 8d 04 06 00
```

## 问题描述

客户需要用我司设备替代华为设备, 在客户原有的环境华为设备上认证获得level3的权限, 替换我司设备后, 登陆设备发现权限很低, 通过dis user-interface 看是level3, 怀疑是采用了华为属性导致的, 没有获得network-admin级别的权限。

## 过程分析

分析有两种解决方法

1. 在客户的free-radius上添加我司的私有属性
2. 直接在思科属性上添加我司设备可以识别的思科属性, 但该方案需要去掉华为属性, 因为客户组网里有华为设备固放弃该方法。

## 解决方法

在客户free-radius服务器上添加我司私有属性步骤

第一步: 在free-radius目录下寻找dictionary.h3c (如果没有需要添加该文件) 然后在该文件下添加

```
ATTRIBUTE H3c-AV-Pair 210 string
```

路径和添加结果如图所示

```

[root@Radius-Access ~]# cat /usr/share/freeradius/dictionary.h3c
# -*- text -*-
# Copyright (C) 2011 The FreeRADIUS Server project and contributors
#####
# Dictionary for Huawei-3Com. See also dictionary.huawei
#
# http://www.h3c.com
#
# $Id$
#####

VENDOR      H3C                25506

BEGIN-VENDOR H3C
ATTRIBUTE   H3c-Input-Peak-Rate      1 integer
ATTRIBUTE   H3c-Input-Average-Rate   2 integer
ATTRIBUTE   H3c-Input-Basic-Rate     3 integer
ATTRIBUTE   H3c-Output-Peak-Rate     4 integer
ATTRIBUTE   H3c-Output-Average-Rate  5 integer
ATTRIBUTE   H3c-Output-Basic-Rate    6 integer
ATTRIBUTE   H3c-Domain-Name          17 string
ATTRIBUTE   H3C-Connect-Id           26 integer
ATTRIBUTE   H3c-Exec-Privilege       29 integer
ATTRIBUTE   H3C-NAS-Startup-Timestamp 59 integer
ATTRIBUTE   H3C-Ip-Host-Addr         60 string
ATTRIBUTE   H3c-VPN-instance         104 string
ATTRIBUTE   H3C-Microsegment-Id      182 string
ATTRIBUTE   H3c-Input-Interval-Octets 201 integer
ATTRIBUTE   H3c-Output-Interval-Octets 202 integer
ATTRIBUTE   H3c-Input-Interval-Packets 203 integer
ATTRIBUTE   H3c-Output-Interval-Packets 204 integer
ATTRIBUTE   H3c-Input-Interval-Gigawords 205 integer
ATTRIBUTE   H3c-Output-Interval-Gigawords 206 integer
ATTRIBUTE   H3c-AV-Pair                210 string
ATTRIBUTE   H3C-Product-ID             255 string
ATTRIBUTE   H3c-Server-String          61 string
ATTRIBUTE   H3C-Ita-Policy             216 string
END-VENDOR H3C

```

第二步：在free-radius目录下找到“dictionary”文件，之后添加以下字符（与其他字典放在一起，不要在最前面或者最后面）

**\$INCLUDE dictionaries/dictionary.h3c**

路径和添加结果如图所示

```

[root@Radius-Access ~]# clear
[root@Radius-Access ~]# ls -l /usr/share/freeradius/
total 1552
-rw-r--r--. 1 root root 631 May 10 2020 audicocodes.bk
-rw-r--r--. 1 root root 8943 Jun 11 2020 dictionary
-rw-r--r--. 1 root root 1499 May 9 2019 dictionary.3com
-rw-r--r--. 1 root root 2346 May 9 2019 dictionary.3gpp
-rw-r--r--. 1 root root 5414 May 9 2019 dictionary.3gpp2
-rw-r--r--. 1 root root 10920 May 9 2019 dictionary.acc
-rw-r--r--. 1 root root 9605 May 9 2019 dictionary.acme
-rw-r--r--. 1 root root 425 May 9 2019 dictionary.actelis
-rw-r--r--. 1 root root 366 May 9 2019 dictionary.adtran
-rw-r--r--. 1 root root 631 May 9 2019 dictionary.aerohive
-rw-r--r--. 1 root root 633 May 9 2019 dictionary.airespace
-rw-r--r--. 1 root root 3652 May 9 2019 dictionary.alcatel
-rw-r--r--. 1 root root 7577 May 9 2019 dictionary.alcatel.esam
-rw-r--r--. 1 root root 3303 May 9 2019 dictionary.alcatel-lucent.aaa
-rw-r--r--. 1 root root 13303 May 9 2019 dictionary.alcatel.sr
-rw-r--r--. 1 root root 964 May 9 2019 dictionary.alteon
-rw-r--r--. 1 root root 7444 May 9 2019 dictionary.altiga
-rw-r--r--. 1 root root 11902 May 9 2019 dictionary.alvarion
-rw-r--r--. 1 root root 1214 May 9 2019 dictionary.alvarion.wimax.v2_2
-rw-r--r--. 1 root root 1134 May 9 2019 dictionary.apc
-rw-r--r--. 1 root root 5589 May 9 2019 dictionary.aptilo
-rw-r--r--. 1 root root 8449 May 9 2019 dictionary.aptis
-rw-r--r--. 1 root root 495 May 9 2019 dictionary.arbor
-rw-r--r--. 1 root root 551 May 9 2019 dictionary.arista
-rw-r--r--. 1 root root 2223 May 9 2019 dictionary.aruba
-rw-r--r--. 1 root root 38943 May 9 2019 dictionary.ascend
-rw-r--r--. 1 root root 20316 May 9 2019 dictionary.ascend.illegal
-rw-r--r--. 1 root root 3105 May 9 2019 dictionary.asn
-rw-r--r--. 1 root root 778 May 10 2020 dictionary.audiocodes
-rw-r--r--. 1 root root 934 May 9 2019 dictionary.avaya
-rw-r--r--. 1 root root 1600 May 9 2019 dictionary.azaire
-rw-r--r--. 1 root root 11907 May 9 2019 dictionary.bay
-rw-r--r--. 1 root root 1621 May 9 2019 dictionary.bintec
-rw-r--r--. 1 root root 735 May 9 2019 dictionary.bluecoat
-rw-r--r--. 1 root root 1523 May 9 2019 dictionary.boingo
-rw-r--r--. 1 root root 484 May 9 2019 dictionary.bristol
-rw-r--r--. 1 root root 17651 May 9 2019 dictionary.broadsoft
-rw-r--r--. 1 root root 688 May 9 2019 dictionary.brocade
-rw-r--r--. 1 root root 657 May 9 2019 dictionary.bskyb
-rw-r--r--. 1 root root 404 May 9 2019 dictionary.bt
-rw-r--r--. 1 root root 8819 May 9 2019 dictionary.cablelabs

```

```

$INCLUDE dictionary.digium
$INCLUDE dictionary.dragonwave
$INCLUDE dictionary.efficientip
$INCLUDE dictionary.eltex
$INCLUDE dictionary.epygi
$INCLUDE dictionary.erx
$INCLUDE dictionary.equallogic
$INCLUDE dictionary.ericsson
$INCLUDE dictionary.ericsson.ab
$INCLUDE dictionary.ericsson.packet.core.networks
$INCLUDE dictionary.extreme
$INCLUDE dictionary.f5
$INCLUDE dictionary.fdxtded
$INCLUDE dictionary.freeradius
$INCLUDE dictionary.freeswitch
$INCLUDE dictionary.fortinet
$INCLUDE dictionary.foundry
$INCLUDE dictionary.gandalf
$INCLUDE dictionary.genie
$INCLUDE dictionary.h3c
$INCLUDE dictionary.hillstone
$INCLUDE dictionary.hp
$INCLUDE dictionary.huawei
$INCLUDE dictionary.iea
$INCLUDE dictionary.infonet
$INCLUDE dictionary.issanni
$INCLUDE dictionary.itk
$INCLUDE dictionary.ipunplugged
$INCLUDE dictionary.juniper
$INCLUDE dictionary.karlnet
$INCLUDE dictionary.kineta

```

第三步：在用户文件中的“用户授权属性”中增加如下授权字段（对于实验室环境是在free-radius添加路径为freeradius/etc/raddb/users，在客户环境是远程数据库，因为涉密没有看到路径）  
添加后的结果如下图所示

<input type="checkbox"/>	Editar	<input type="checkbox"/>	Copiar	<input type="checkbox"/>	Borrar	1303	W_PL-PRUEBAS	H3c-AV-Pair	=	shell roles=network-admin
<input type="checkbox"/>	Editar	<input type="checkbox"/>	Copiar	<input type="checkbox"/>	Borrar	1304	R_PL-PRUEBAS	H3c-AV-Pair	=	shell roles=network-admin
<input type="checkbox"/>	Editar	<input type="checkbox"/>	Copiar	<input type="checkbox"/>	Borrar	1305	R_PL-PRUEBAS	H3c-AV-Pair	=	shell roles=network-operator

第四步：做完所有的操作后需要重启Free-radius软件

第五步：打开debug radius packet，SSH触发认证后检查H3C属性是否生效。使用display users 查看用户获取的权限是否为“network-admin”

正确结果debug日志如下图所示

```

~^
*Apr 23 21:31:52:718 2024 H3C_PRUEBAS
RADIUS/7/EVENT: Sent request packet and create
request context successfully.
*Apr 23 21:31:52:718 2024 H3C_PRUEBAS
RADIUS/7/EVENT: Added request context to global
table successfully.
*Apr 23 21:31:52:718 2024 H3C_PRUEBAS
RADIUS/7/EVENT: Processing AAA request data.
*Apr 23 21:31:52:722 2024 H3C_PRUEBAS
RADIUS/7/EVENT: Reply SocketFd recieved EPOLLIN
event.
*Apr 23 21:31:52:722 2024 H3C_PRUEBAS
RADIUS/7/EVENT: Received reply packet
succuessfully.
*Apr 23 21:31:52:723 2024 H3C_PRUEBAS
RADIUS/7/EVENT: Found request context, dstIP:
10.20.252.4, dstPort: 1812, VPN instance: --
(public), socketFd: 40, pktID: 43.
*Apr 23 21:31:52:723 2024 H3C_PRUEBAS
RADIUS/7/EVENT: The reply packet is valid.
*Apr 23 21:31:52:724 2024 H3C_PRUEBAS
RADIUS/7/EVENT: Decoded reply packet successfully.
*Apr 23 21:31:52:724 2024 H3C_PRUEBAS
RADIUS/7/PACKET:
    H3c-AVPair="shell:roles=network-admin"
*Apr 23 21:31:52:725 2024 H3C_PRUEBAS
RADIUS/7/PACKET:
    02 2b 00 35 89 e8 11 1f d2 31 e0 8d 12 53 11 19
    30 ce 9e 85 1a 21 00 00 63 a2 d2 1b 73 68 65 6c
    6c 3a 72 6f 6c 65 73 3d 6e 65 74 77 6f 72 6b 2d

```

### 注意事项

Free-radius重启会导致几分钟的认证业务中断，重启前确认有备份文件再重启