防火墙管理员通过radius认证登录后闪退

AAA 李超 2022-06-29 发表

组网及说明

不涉及

告警信息

不涉及

问题描述

现场防火墙的管理员计划通过radius实现认证，认证通过后才可以登录防火墙，测试时发现，当用户登录防火墙后，立即闪退出去

```
<F1070-IRF>ssh 172.31.0.19
Username: dxl
Press CTRL+C to abort.
Connecting to 172.31.0.19 port 22.
dxl@172.31.0.19's password:
Enter a character ~ and a dot to abort.

******************************************************************************
* Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************


Connection to 172.31.0.19 closed.
<F1070-IRF>
```

过程分析

设备上关键配置如下：

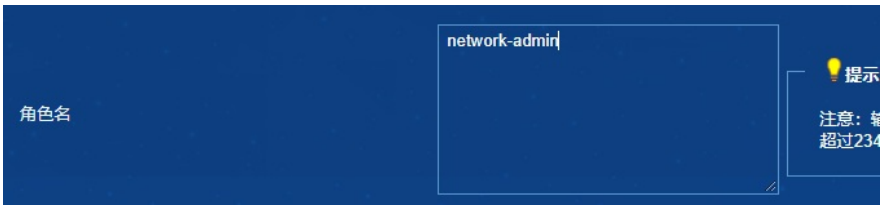
```
#
radius scheme aaa
primary authentication 172.31.0.95 vpn-instance management
primary accounting 172.31.0.95 vpn-instance management
key authentication cipher $c$3$w30tobD7VrfpTjG1AggmaUeLnrHng4ZvTLRkOg==
key accounting cipher $c$3$lS3geNGU+vAVGiQzBUb01uEWavt5HSZb860E8Q==
 user-name-format without-domain
 nas-ip 172.31.0.19
#
domain bbb
 authentication login local radius-scheme aaa
 authorization login local radius-scheme aaa
 accounting login none
#
 domain default enable bbb
#
```

通过在防火墙debug发现，radius服务器回包中没有关于用户角色的信息，导致用户未授权退出

```
*Jan 26 03:37:24:228 2010 M9006 RADIUS/7/EVENT:
Sent request packet and create request context successfully.
*Jan 26 03:37:24:228 2010 M9006 RADIUS/7/EVENT:
Added request context to global table successfully.
*Jan 26 03:37:24:228 2010 M9006 RADIUS/7/EVENT:
Processing AAA request data.
*Jan 26 03:37:24:465 2010 M9006 RADIUS/7/EVENT:
Reply SocketFd received EPOLLIN event.
*Jan 26 03:37:24:465 2010 M9006 RADIUS/7/EVENT:
Received reply packet successfully.
*Jan 26 03:37:24:466 2010 M9006 RADIUS/7/EVENT:
Found request context, dstIP: 172.31.0.95, dstPort: 1812, VPN instance: management, socketFd: 38, pktID: 192.
*Jan 26 03:37:24:466 2010 M9006 RADIUS/7/EVENT:
The reply packet is valid.
*Jan 26 03:37:24:467 2010 M9006 RADIUS/7/EVENT:
Decoded reply packet successfully.
*Jan 26 03:37:24:467 2010 M9006 RADIUS/7/PACKET:
    Service-Type=Login-User
    Session-Timeout=86400
*Jan 26 03:37:24:468 2010 M9006 RADIUS/7/PACKET:
 02 c0 00 20 f7 9a 8e b6 72 a3 95 a8 df 08 55 89
 8b 67 3d fd 06 06 00 00 00 01 1b 06 00 01 51 80

*Jan 26 03:37:24:468 2010 M9006 RADIUS/7/EVENT:
Sent reply message successfully.
*Jan 26 03:37:24:468 2010 M9006 RADIUS/7/EVENT:
PAM_RADIUS: Fetched authentication reply-data successfully, resultCode: 0
*Jan 26 03:37:24:469 2010 M9006 RADIUS/7/EVENT:
```

在imc上对应的用户中增加network-admin角色后，登录正常




```
*Jan 26 03:29:47:408 2010 M9006 RADIUS/7/EVENT:
Found request context, dstIP: 172.31.0.95, dstPort: 1812, VPN instance: management, so
*Jan 26 03:29:47:408 2010 M9006 RADIUS/7/EVENT:
The reply packet is valid.
*Jan 26 03:29:47:408 2010 M9006 RADIUS/7/EVENT:
Decoded reply packet successfully.
*Jan 26 03:29:47:409 2010 M9006 RADIUS/7/PACKET:
    Service-Type=Login-User
    Session-Timeout=86400
    H3c-User-Roles="shell:roles="network-admin""
```

解决方法

在imc的用户>设备管理用户>设备管理用户>修改设备管理用户视图下修改角色名为network-admin后解决