

知 iMC Radius dot1x自动下线排查

802.1X iMC Radius skei 2024-04-24 发表

问题描述

背景: 典型iMC结合MS-CHAPV2认证方案上线, 用户端安装inode认证

问题: 用户上线后, 约50秒自动断线

过程分析

排查: debug dot1x, 属于用户下线类别

交换机 dot1x认证错误码含义:

802.1x error code含义:

- 1 客户端主动下线 */
- 2 埠状态错误 */
- 3 客户端重启 */
- 4 重认证失败 */
- 5 设备强制去授权 */
- 6 埠重启 */
- 7 管理员将接口shutdown(公有最后一个) */
- 8 用户名和密码不对 */
- 9 握手失联 */
- 10 闲置切断 */
- 11 限制切断 */
- 12 服务器发起的切断 */
- 13 实时计费失败 */
- 14 缺省错误 */

```
%Jan 5 23:07:29:949 2013 sw2 DOT1X/6/DOT1X_LOGOFF: -ifName=GigabitEthernet1/0/5-MACAddr=e4a8-dfa4-d4f8-VLANID=1-Username=localuser01-ErrCode=1: 802.1x user was logged off.
%Jan 5 23:07:29:949 2013 sw2 DOT1X/7/PACKET:
Transmitted a packet on Interface GigabitEthernet1/0/5.
Destination Mac Address=e4a8-dfa4-d4f8
Source Mac Address=9ce8-953c-d194
VLAN ID=5
Mac Frame Type=888e
Protocol Version ID=1
Packet Type=0
Packet Length=4
-----Packet Body-----
Code=4
Identifier=a
Length=1024
%Jan 5 23:07:29:949 2013 sw2 DOT1X/7/EVENT: PAE is in Disconnect state: UserMAC=e4a8-dfa4-d4f8, VL
ANTD=1, Interface=GigabitEthernet1/0/5
%Jan 5 23:07:29:949 2013 sw2 DOT1X/7/EVENT: Interface GigabitEthernet1/0/5 received Set the port a
uthorization status to unauthorized event.
%Jan 5 23:07:29:962 2013 sw2 DOT1X/7/EVENT: Sent accounting-stop request: UserMAC=e4a8-dfa4-d4f8,
```

查看 inode 离线原因:



再排查网络, 用户端上线后的IP和iMC服务器IP不可达(组网特别原因), 因为iMC 网关在CoreSW上, 但用户IP GW不在, 路由不可达

解决方法

解法方法: 在iMC服务器添加用户路由成功解决相关问题

注：下线原因的值 1 到 57 是标准属性，NAS 通过计费结束的 Acct-Terminate-Cause(49)属性上传给 UAM，UAM 写入接入明细“下线原因”字段。255 到 260，是扩展属性，UAM 直接写入接入明细“下线原因”字段。

1.1 User request 1

表 1-1 产生 User request 的原因及处理建议

| | |
|------|---|
| 描述 | 表示用户主动下线。 Acct-Terminate-Cause(49) = 1 |
| 可能原因 | <ul style="list-style-type: none">情况一：用户手工点击连接中的“断开”主动下线。情况二：在启用策略服务器的情况下，iNode 客户端与策略服务器不通造成、iNode 与策略服务器的心跳超时后主动下线。 |
| 处理建议 | 对于情况二，iNode 通常会给出类似“代理服务没有响应，即将强行下线”之类的提示。这种请检查 iNode 与策略服务器是否路由可达，可以通过 ping、tracert 等诊断命令来排查。如果 iNode 与策略服务器路由可达，请检查 iNode 与策略服务器通信的端口（UDP 9019）是否被防火墙过滤，包括客户端 PC 上的软件防火墙，网络中的防火墙及 UAM 服务器上的软件防火墙。 |