

组网及说明

现场有两台认证服务器，一台装imc，另一台装了逃生工具，认证点在交换机上

问题描述

现场V5的交换机可以逃生成功，但是有一台V7交换机逃生不成功，如果做正常1x认证是可以认证成功的，且V7交换机和两台认证服务器都是可以ping通的

过程分析

对于设备侧来说，结合逃生工具的逃生没有什么特殊配置，只需要配置primary和secondary认证服务器即可，查看配置未发现问题，确认密钥配置也是正确的

```
#
dot1x
dot1x authentication-method pap
# radius scheme imc
primary authentication 192.168.254.x
primary accounting 192.168.254.x
secondary authentication 192.168.2.x
secondary accounting 192.168.2.x
key authentication cipher $c$3$EWHuk0HFfOTpWMRp36F6SL7QO3O0fdOmVehwrQ==
key accounting cipher $c$3$MLuGr0dyZld3YdDlxh1bT2sJSzXX50fukZtrLg==
user-name-format without-domain
```

```
#
domain ead
authentication lan-access radius-scheme imc
authorization lan-access radius-scheme imc
accounting lan-access radius-scheme imc
```

```
#
domain default enable ead
在设备侧debug radius查看radius交互过程报文
```

从debug里面看，确实探测到主服务器192.168.254.x不可达了，尝试三次后切换到备服务器

```
*Jan 22 00:18:56:548 2013 H3CS5130_5A105 RADIUS/7/EVENT: Retransmitting request packet, currentTries: 3, maxTries: 3.
```

```
*Jan 22 00:18:59:548 2013 H3CS5130_5A105 RADIUS/7/EVENT: Response timed out.
```

```
*Jan 22 00:18:59:548 2013 H3CS5130_5A105 RADIUS/7/EVENT: Found request context, dstIP: 192.168.254.x; dstPort: 1813; VPN instance: --(public); socketfd: 70; pktID:206.
```

```
*Jan 22 00:18:59:548 2013 H3CS5130_5A105 RADIUS/7/EVENT: Reached the maximum retries.
```

```
*Jan 22 00:18:59:549 2013 H3CS5130_5A105 RADIUS/7/EVENT: Set status of server to block successfully. serverIP: 192.168.254.x, serverPort: 1813.
```

```
*Jan 22 00:18:59:549 2013 H3CS5130_5A105 RADIUS/7/EVENT: Got next server successfully. serverIP: 192.168.2.x; serverPort: 1813.
```

然后给备imc发送aaa请求数据，没有收到回复，尝试三次没响应之后，server置为block状态。

```
*Jan 22 00:19:03:073 2013 H3CS5130_5A105 RADIUS/7/EVENT: Processing AAA request data.
```

```
*Jan 22 00:19:05:548 2013 H3CS5130_5A105 RADIUS/7/EVENT: Response timed out.
```

```
*Jan 22 00:19:08:549 2013 H3CS5130_5A105 RADIUS/7/EVENT: Reached the maximum retries.
```

```
*Jan 22 00:19:08:551 2013 H3CS5130_5A105 RADIUS/7/EVENT: Received status of server changing event.
```

```
*Jan 22 00:19:08:552 2013 H3CS5130_5A105 RADIUS/7/EVENT: Aaad sent notification about the change of server status to application process successfully. Server state: block.
```

```
*Jan 22 00:19:08:553 2013 H3CS5130_5A105 RADIUS/7/EVENT: Set status of server to block successfully. serverIP: 192.168.2.x, serverPort: 1813.
```

```
*Jan 22 00:19:08:554 2013 H3CS5130_5A105 RADIUS/7/EVENT: Got next server failed.
```

```
*Jan 22 00:19:08:555 2013 H3CS5130_5A105 RADIUS/7/EVENT: RESEND_RADIUS: Send stop-accounting message to AAA.
```

```
*Jan 22 00:19:08:555 2013 H3CS5130_5A105 RADIUS/7/EVENT: RESEND_RADIUS: Ready to resend stop-accounting packet SessiOnID= 00000004201301220016360000043708100179.
```

看secondary服务器有回包，但是设备侧判断报文是无效的，怀疑是服务器侧问题

```
*Jan 22 00:19:12:559 2013 H3CS5130_5A105 RADIUS/7/EVENT: Found request context, dstIP: 192.168.2.x, dstPort: 1812, VPN instance: --(public), socketFd: 70, pktID: 167.
```

```
*Jan 22 00:19:12:560 2013 H3CS5130_5A105 RADIUS/7/ERROR: Reply packet: Invalid packet
```

authenticator.

*Jan 22 00:19:12:560 2013 H3CS5130_5A105 RADIUS/7/ERROR: The reply packet is invalid.

解决方法

联系服务器侧排查后发现，当前服务器逃生工具安装目录 /RADIUSFailOpen/etc 下的clients没有包含该台交换机，现场将 iMC UAM/ iMC EIA 后台服务器上 iMC 安装路径 /uam/etc/clients 文件拷贝到当前服务器逃生工具安装目录 /RADIUSFailOpen/etc 下后问题解决