iMC EIA Portal认证下线原因为Online Check的典型问题分析

马光彬　2017-12-14 发表

portal认证，无线网络正常连接，个别用户不定时掉线，有时两个小时左右，有时不到一小时就会掉线，需要重新进行protal认证。通过查看接入明细，发现用户下线原因是Online Check（检查在线记录）。

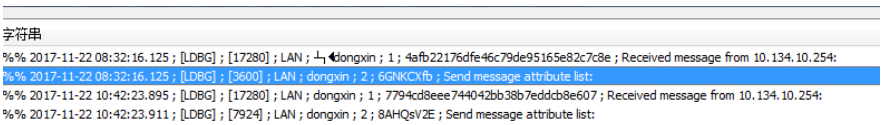
帐号名	liyueliang	用户姓名	李悦亮
服务名	yonghumingrenzheng	用户分组	群团综合管理科
登录名	50:8F:4C:68:53:ED	接入策略名	renzheng

接入信息

接入开始时间	2017-11-17 12:21:24	接入结束时间	2017-11-18 13:00:00
接入时长	24小时38分钟36秒	下线原因	Online Check（检查在线纪录）
设备IP地址	10.134.10.254	设备端口号	0
设备槽号	2	设备子槽号	0
设备序列号		IMSI号码	50-8F-4C-68-53-ED
上传字节数	0	下载字节数	0
VLAN ID/内层VLAN ID	200	外层VLAN ID	
无线SSID	TJport	NAS ID	WX3520H
Windows域		用户IP地址	10.134.2.1
用户MAC地址	50:8F:4C:68:53:ED	设备NAT IP地址	10.134.10.254
客户端版本号		代理类型	设备至本地
计费会话标识	00000007201711171220180000026ac16100308	终端类型	
终端厂商	XIAOMI	终端操作系统	Android
IMEI号码			

1、某些情况下UAM收不到设备的计费更新报文，比如认证设备与UAM之前的路由有问题，比如设备重启（设备上没有配置accounting-on），这时为了避免用户在UAM上挂死，UAM在如下图所示的老化时间时没有任何认证设备关于该账号的计费更新报文，则UAM将该用户的在线表清除，同时在接入明细中标识该用户的下线原因为online-check。

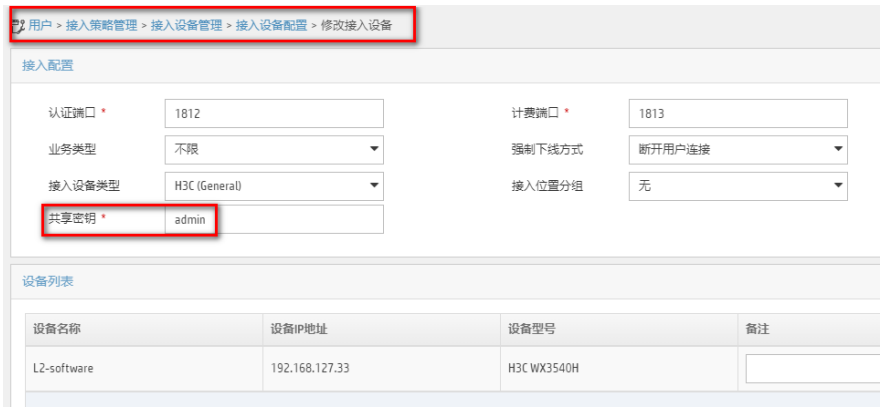
2、收集并分析UAM调试日志，发现iMC没有收到计费报文。



3、查看设备上radius方案和domain域下是否配置了accouting相关命令。配合iMC EIA组件做认证，必须配置accounting相关命令，这样才能正常完成整个认证过程。

```
#
radius scheme portal
 primary authentication 192.168.127.97
 primary accounting 192.168.127.97
 key authentication cipher $c$3$GQGIWRVqV7LJ7+yE8S/1A25jpAA1jh26
 key accounting cipher $c$3$I/JwExDcr25B69HJquEVVGoPRLwNr50q
 nas-ip 192.168.127.33
#
domain portal
 authentication portal radius-scheme portal
 authorization portal radius-scheme portal
 accounting portal radius-scheme portal
#
```

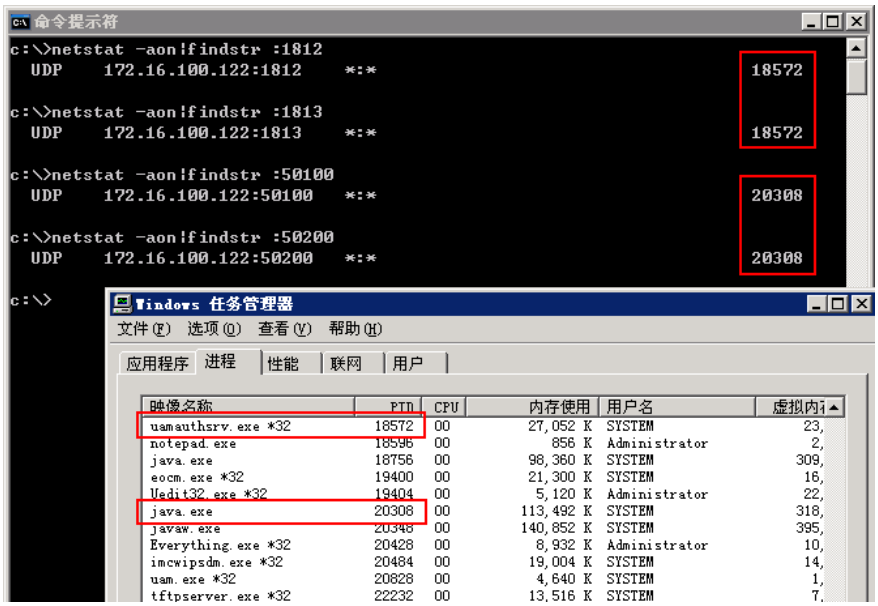
4、检查计费密钥是否跟iMC侧一致，建议修改测试。



说明：密钥缺省是密文显示，可以通过修改参数显示为明文。进入用户>接入策略管理>业务参数配置>系统配置>系统参数配置，修改“密钥显示方式”为“明文”即可。

5、检查nas设备与iMC通信的UDP 1813端口是否正常，计费报文使用UDP 1813端口，需要保证该端口正常通信。

6、检查iMC侧是否有防火墙或杀毒软件阻隔UDP 1813端口，或者其他程序占用UDP 1813端口，正常情况下1813 UDP端口是被uam相关进程所监听。



说明：Windows操作系统中，通过

netstat –aon|findstr :端口号

命令来显示某一端口的监听状态及其对应的进程PID

举例，对于命令提示符回显：

其中第一列UDP所指监听的协议，第二列172.16.100.122:1812所指监听的服务器的IP和端口号，第三列*:*代表此行信息为监听状态，最右一列8780代表此协议监听的进程PID。查到端口所对应的进程PID后，请查看Windows任务管理器，1812/1813端口所对应的应为uam相关的进程。

设备上radius方案和domain域下配置accouting相关命令，并保证密钥与iMC侧一致，问题解决。

收集信息

1. BAS设备型号版本，iMC版本；
2. BAS设备配置，iMC所有相关配置截图；
3. 设备上的debug portal packet,debug radius packet输出；
4. 认证所用的用户名，终端IP地址，认证时间点，掉线时间点，接入明细截图
5. iMC服务器上的UAM调试日志和portal调试日志；

UAM调试日志收集方法

先在用户-接入策略管理-业务参数配置-系统配置-UAM运行日志参数配置中将日志级别设为“调试”，如下图：

然后复现问题测试，完成后反馈iMC安装目录imc\uam\log\目录下以当天日期为名的文件。（如果UAM是分布式部署，那么此日志位于UAM所在的从服务器上）如下图：

Portal调试日志收集方法

先在用户-接入策略管理-portal服务管理-服务器配置页面将日志级别设为“调试”，如下图：

然后复现问题测试，完成后反馈iMC安装目录imc\portal\logs\目录下的portalserver文件。如下图：