

解决iMC EIA用户上线几分钟之后自动下线的经验案例

李树兵 2018-01-09 发表

某局点用户进行Portal认证，发现认证上来的用户接入时长几乎全部都是2分钟。如下图所示：

用户 > 用户接入日志 > 接入明细

接入明细查询

帐号名: 139139 用户分组: 接入开始时间 从: 2018-01-02 12:31 至: 2018-01-09 12:31 接入结束时间 从: 至:

定制界面

帐号名	用户姓名	登录名	服务名	接入开始时间	接入时长	用户IP地址
139139	139139	D4F46F	pukou-weixin	2018-01-09 11:53:13	2分钟 1秒	10.10.104.181
139139	139139	D4F46F	pukou-weixin	2018-01-09 11:51:10	2分钟 1秒	10.10.104.181
139139	139139	13913918	pukou-weixin	2018-01-09 11:48:47	2分钟 1秒	10.10.104.181
139139	139139	D4F46F	pukou-weixin	2018-01-08 11:48:27	2分钟 1秒	10.10.104.181

171 0 版权所有 © 2007-2016 杭州华三通信技术有限公司，保留一切权利。

用户上线2分钟之后自动下线，重新认证。

复现问题，收集认证过程中的UAM以及portal调试级别的日志，通过日志可以发现日志中记录如下信息：

```
%% 2018-01-09 11:55:34.203 ; [LDBG] ; [19624] ; radDispatcher ; prsRawPkt: chk-sum 1735778518.
%% 2018-01-09 11:55:34.203 ; [LDBG] ; [19624] ; LAN ; prsMixedUsr: in [60:91:F3:0D:D9:E2], out [6
0:91:F3:0D:D9:E2]. %% 2018-01-09 11:55:34.203 ; [LDBG] ; [19624] ; radEnt ; setPxyType: No
domain name. %% 2018-01-09 11:55:34.203 ; [LDBG] ; [22192] ; LAN ; lanAcctMsgProc.exec: begin.
%% 2018-01-09 11:55:34.203 ; [LDBG] ; [22192] ; USR ; chkIfTransparentAuthUsr:
[60:91:f3:0d:d9:e2] is allowed to do transparent auth as user [1876160xxxx]. %% 2018-01-09
11:55:34.203 ; [LDBG] ; [22192] ; LAN ; lanAcctUpd.exec: Begin. %% 2018-01-09 11:55:34.203 ; [LD
BGG] ; [22192] ; lanAcctUpd ; getUpdInfoByOnline: usrSrv[1876160xxxx], nasIp[168427542], acctSes
s[000000072018010911443400137c6308100971], usrid[20417], srvcl[20420]. %% 2018-01-09 11:5
5:34.203 ; [LDBG] ; [22192] ; LAN ; c.getUsrSrvInfoById: begin. %% 2018-01-09 11:55:34.203 ; [LD
BGG] ; [22192] ; accSvc ; queryServiceStrategyById: matching rule(1) with priority 0 under srv-templ
. %% 2018-01-09 11:55:34.203 ; [LDBG] ; [22192] ; LAN ; c.getUsrSrvInfoById: end OK. %% 2018-0
1-09 11:55:34.203 ; [LDBG] ; [22192] ; LAN ; lanAcctUpd.acctSrvChk: doing chkBlacklist OK. %% 20
18-01-09 11:55:34.203 ; [WARN] ; [22192] ; LAN ; UsrSvc.calcUsrSessQuan: user[id:20417] is out of
online time limit. //日志记录id为20417的用户超过了在线时间限制 %% 2018-01-09 11:55:34.203 ; [WA
RN] ; [22192] ; LAN ; lanAcctUpd.acctSrvChk: fail to call usrSvc.calcUsrSessQuantity. errCode:
63639. %% 2018-01-09 11:55:34.203 ; [ERR] ; [22192] ; LAN ; lanAcctUpd.execCharging: Fail to call
acctSrvCheck. errCode: 63639 %% 2018-01-09 11:55:34.203 ; [ERR] ; [22192] ; LAN ; lanAcctUpd.e
xec: failed to exec charging, errCode: 63639. %% 2018-01-09 11:55:34.203 ; [LDBG] ; [22192] ; LAN
; lanAcctUpd.exec: End OK. %% 2018-01-09 11:55:34.203 ; [LDBG] ; [22192] ; accSvc ; matchSvcStr
agy: matching default rule(1) under srv-templ. %% 2018-01-09 11:55:34.203 ; [LDBG] ; [22192] ; L
AN ; Begin replyPrivateAttr, auth step is 3, AttrPolicyId is -1, DeviceTypeId is 1100 %% 2018-01-09 1
1:55:34.203 ; [LDBG] ; [22192] ; LAN ; 1876160xxxx ; 5 ; 7800f40123cb41e5a66de566d4bb1ecf ; OE
aJOEOw ; Send message attribute list: Code = 5 ID = 177 ATTRIBUTES: Session-Timeout(27) = 0
%% 2018-01-09 11:55:34.203 ; [LDBG] ; [22192] ; LAN ; lanAcctMsgProc.exec: End. %% 2018-01-09
11:55:34.462 ; [LDBG] ; [19624] ; LAN ; 44:6E:E5:9B:6C:CE ; 4 ;
3d2dcc50e614464da8a8c4102be110b7 ; Received message from 10.10.0.22: CODE = 4. ID = 178.
ATTRIBUTES: User-Name(1) = "44:6E:E5:9B:6C:CE". NAS-Identifier(32) = "JS-NJ-PKQZF.WX5560
H". NAS-Port(5) = 16777251. NAS-Port-Type(61) = 19. NAS-Port-Id(87) = "0100000000000035". NA
S-IP-Address(4) = 168427542. Framed-Protocol(7) = 255. Calling-Station-Id(31) = "44-6E-E5-9B-6C-
CE". Called-Station-Id(30) = "70-3D-15-9A-22-E0:PUKOU-WIFI". Framed-IP-Address(8) =
168455263. Acct-Session-Id(44) = "000000072018010911443400137c6108100971". Acct-Session-Ti
me(46) = 121. Acct-Input-Octets(42) = 1064820. Acct-Output-Octets(43) = 48004107. Acct-Input-Pac
kets(47) = 8405. Acct-Output-Packets(48) = 36455. Acct-Input-Gigawords(52) = 0. Acct-Output-Giga
words(53) = 0. Acct-Terminate-Cause(49) = 5. Class(25) = "BA2jNxnI". hw_IP_Host_Addr(60) = "10.1
0.108.95 44:6e:e5:9b:6c:ce". Acct-Authentic(45) = 1. H3C_DHCP_Option55(208) = "012103060f1a1c
333a3b". Acct-Status-Type(40) = 2. //之后设备发送给iMC服务器的CODE 4报文中就要求结束计费，
用户下线。 Acct-Delay-Time(41) = 0. Event-Timestamp(55) = 1515498395. hw_Product_ID(255) = "
H3C WX5560H". hw_Nas_Startup_Timetamp(59) = 1514070786.
```

通过日志可以看出为某个地方配置用户在线时间限制导致用户达到时间之后下线。

检查接入策略配置中单次最大在线时长的配置，看到现场接入策略配置的单次最大在线时长为2分钟，此为导致用户上线2分钟之后自动下线的的原因，将此数值去掉，采用空配置，用户重新登录问题解决。

Port Center

默认视图 admin 桌面版 帮助 关于

用户 业务 告警 报表 系统管理

通用搜索

接入策略

接入时段: 无

下行速率(Kbps):

优先级:

首选EAP类型: EAP-MD5

EAP自协商: 启用

下发地址池:

分配IP地址: 否

上行速率(Kbps):

下发用户组:

单次最大在线时长(分钟): 2

下发VLAN:

☐ 下发User Profile

☐ 下发ACL

导致用户上线一段时间之后自动下线的的原因可能有如下几方面：

第一方面：iMC侧端口组信息管理里面的心跳间隔和心跳超时设置了时间，因为移动端（手机终端）的浏览器无法记录后台信息，也就是终端无法和iMC的portalserver服务器交互心跳报文，这样就会导致心跳超时时间之后用户下线。所以在有移动终端的组网环境下，建议端口组信息配置中心心跳间隔和心跳超时设置为0，及不进行心跳检测。

首页 资源 用户 业务 告警 报表 系统管理

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 端口组信息配置 > 增加端口组信息

增加端口组信息

基本信息

端口组名: 认证方式: PAP认证

无感知认证: 不支持

IP地址组: 20

页面推送策略: 缺省认证页面

高级信息

开始端口: 0

终止端口: ZZZZZZ

协议类型: HTTP

快速认证: 否

是否NAT: 否

错误透传: 是

提示语言: 动态检测

客户端防破解: 否

心跳间隔(分钟): 0

心跳超时(分钟): 0

用户域名: 端口组描述:

第二方面：设备侧domain域下配置了idle-cut的配置。在设备侧对用户在线情况进行检测，如下面的配置：

domain portal

authorization-attribute idle-cut 29 1024 //检测用户在29分钟之内流量如果小于1024KB的话，设备侧将用户踢下线，同时通知iMC服务器将用户下线。

authentication portal radius-scheme portal

authorization portal radius-scheme portal

accounting portal radius-scheme portal

第三方面：正如此案例中由于误操作在接入策略中配置了单次最大在线时长，此配置常用于微信认证放通临时用户，所以一般不建议配置此选项。

注意：排除以上三个原因如还不能定位问题需要收集信息进行分析。信息包括：认证用户名，下线原因和下线时间以及此过程中的UAM和Portal的调试级别日志，收集完信息之后请联系华三工程师进行分析。

收集日志的方法如下：

较新版本登录到系统管理--系统配置--日志配置，设置uam和portlserver进程为debug级别，之后复现问题，复现之后点击旁边的下载进行日志收集。

系统管理 > 日志配置				
刷新 将日志级别修改为DEBUG可能会影响系统的效率, 请谨慎操作。				
进程名	描述	日志级别	下载日志(当天)	IMF日志
uamThirdAuth		INFO	下载	无
uamjob			下载	无
uam		DEBUG	下载	无
tam		WARN	下载	无
portalserver		DEBUG	下载	无
policyserver		INFO	下载	无
netconf		INFO	下载	无
jserver	本系统启动、访问日志	INFO	下载	无
img	本系统前后台通信消息日志		下载	无

教老版本需要手动设置UAM和Portal的级别为debug，然后登录到服务器后台收集文件。
 UAM日志收集：用户--接入策略管理--业务参数配置--系统配置--UAM运行参数配置，将日志级别设置为调试，然后点击确定生效，之后复现问题。

用户管理

接入用户管理

访客管理

终端管理

用户接入日志

接入策略管理

快速入门

接入服务管理

接入策略管理

接入条件管理

接入设备管理

LDAP业务管理

Portal服务管理

业务参数配置

第三方认证配置

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

UAM运行日志参数配置

日志级别 *

调试

日志保留时长(天) *

30

确定

取消

登录服务器后台，找到iMC安装目录/uam/log文件夹，找到当天日期命名的文件。

D:\Program Files\iMC\uam\log				
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)				
地址(D) D:\Program Files\iMC\uam\log				
名称	大小	类型	修改日期	
20111117.log	1,096 KB	文本文档	2011-11-17	
PLAT_LOG_20111117.log	200 KB	文本文档	2011-11-17	
PLAT_LOG_20111116.log	186 KB	文本文档	2011-11-17	
20111116.log	1,293 KB	文本文档	2011-11-16	

Portal日志收集：用户--接入策略管理--Portal服务管理--服务器配置，在基本信息里面将日志级别改为调试级别，然后点击确定生效，之后复现问题。

Portal服务器配置

基本信息

日志级别 *

调试

Portal Server

原文请求超时时长(秒) *

4

原文心跳间隔时长(秒) *

20

用户心跳间隔时长(分钟) *

5

LB设备地址

Portal Web

请求原文超时时长(秒) *

15

交互原文编码

校验并请求原文

是

使用缓存

是

HTTP页面展示方式

新页面

HTTPS页面展示方式

原页面

Portal主页

http://192.168.10.12:8080/portal/

https://192.168.10.12:8443/portal/

登录服务器后台，找到iMC安装目录/portal/log文件夹，找到portalserver_当天日期的文件。

地址 (D:) D:\Program Files\iMC\portal\logs			
名称	大小	类型	修
2011-08.zip	998 KB	WinRAR ZIP 压缩...	201
2011-09.zip	1,191 KB	WinRAR ZIP 压缩...	201
2011-10.zip	2,430 KB	WinRAR ZIP 压缩...	201
2011-11.zip	90 KB	WinRAR ZIP 压缩...	201
portal web imcserver 2011-11-17.log	1 KB	文本文档	201
portalserver_2011-11-17.txt	2 KB	文本文档	201
standardServer_bootstrap.log	53,765 KB	文本文档	201
timer.2011-11-17.txt	1 KB	文本文档	201