

按终端类型匹配接入策略匹配异常

iMC 汤祺 2019-12-05 发表

组网及说明

现场需求：XP操作系统PC禁止接入网络当中，其余操作系统终端可正常接入网络中。

问题描述

在EIA接入服务接入场景中设置了接入条件去匹配终端操作系统，接入策略则设置为禁止接入，但现场使用xp操作系统PC进行认证后，匹配到了默认策略，正常接入网络中，策略匹配异常。

过程分析

1、终端识别并根据终端类型使用不同策略是需要使用到EIP授权，此时需先检查现场环境是否有注册EIP授权。

名称	版本	允许管理最大终端单元数	允许管理最大物联网模块数	生效日期
业务服务管理	iMC BSM 7.3 (E0501P14)	0	0	2020-2-27
移动办公管理 (IES-SDK已授权)	iMC EMO 7.3 (E0510)	允许终端数：200	0	2020-2-27
应用管理	iMC APM 7.3 (E0501P17)	可管理的应用数量：100	12	2020-2-27
用户行为审计	iMC UBA 7.3 (E0505)	允许最大在线用户数：1000	0	2020-2-27
智能门户管理	iMC IPM 7.3 (E0514)	允许管理最大用户数量：600	0	2020-2-27
终端智能接入管理	iMC EIA 7.3 (E0512H01)	允许最大数：400	2	2020-2-27
终端智能识别管理	iMC EIP 7.3 (E0512H01)	允许最大识别终端数：600	0	2020-2-27

2、EIP授权正常后，检查接入条件中终端操作系统分组设置是否正确

基本配置

服务名：test

业务分组：未分组

缺省安全策略：test

缺省私有属性下发策略：不使用

缺省单帐号最大并发连接数：255

服务描述：可申请

缺省接入策略：access-policy

缺省内网外连策略：不使用

缺省单帐号在线数限制：无限制认证

名称	接入策略	安全策略	私有属性下发策略
test	禁止接入	不使用	不使用

修改接入场景 - Mozilla Firefox

接入时段策略：不限

接入位置分组：不限

SSID分组：不限

终端IP地址分组：不限

终端MAC地址分组：不限

终端厂商分组：不限

终端类型分组：不限

终端操作系统分组：xp

AP分组：不限

接入策略：禁止接入

单帐号最大绑定终端数：10

单帐号在线数限制：10

3、接入策略配置正确后，检查上线成功后该终端管理里终端识别的操作系统类型是否为xp系统

修改终端操作系统分组

基本信息

终端操作系统分组：xp

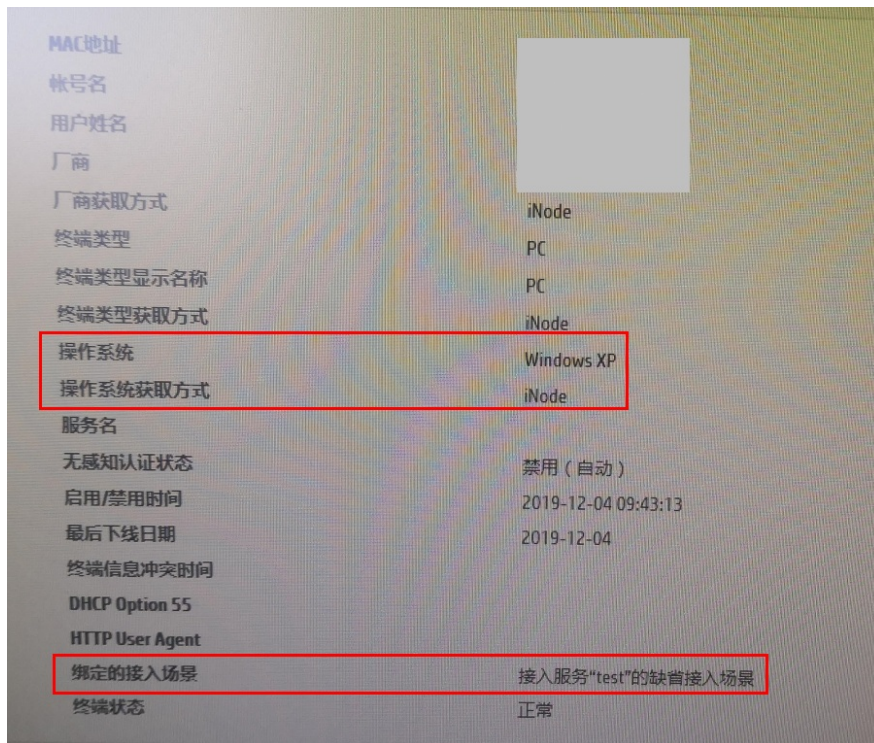
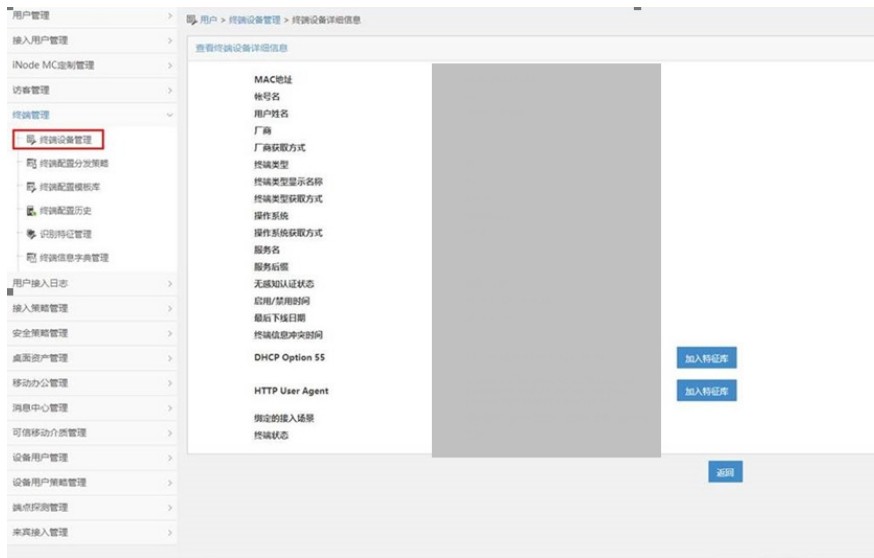
描述：xp

业务分组：未分组

操作策略列表

共有2条记录

操作策略	描述
Windows	Windows操作系统
Windows XP	Windows XP操作系统



终端管理中该终端为通过inode进行认证上线，且正常识别操作系统类型为xp，但实际未匹配到接入场景里的接入策略，而是使用接入服务里的缺省策略认证上线。

以上配置检查完成后，确认配置皆无异常，操作系统类型也正常识别后，可通过查看EIA的debug日志进行确认。

```
%% 2019-12-04 10:52:50.120; [LDBG]; [16964]; LAN; bDILFRABZncuHhIrLVMrfjb1TEM= 111; 1; 65c19233979b4cbfb10275f3c3067d32; Received message from 21.44.60.153:
```

CODE = 1.

ID = 73.

ATTRIBUTES:

User-Name(1) = "..bDILFRABZncuHhIrLVMrfjb1TEM= 111".

Password(2) = "\$\$\$".

NAS-IP-Address(4) = 355220633.

NAS-Identifier(32) = "B-HLHRA-PORTAL-DS01".

NAS-Port(5) = 0.

NAS-Port-Id(87) = "0000000000000000".

NAS-Port-Type(61) = 15.

Service-Type(6) = 2.

Framed-Protocol(7) = 255.

Calling-Station-Id(31) = "00-00-00-00-00-00". (终端mac地址携带属性，可发现该属性携带的mac地址为空)

Acct-Session-Id(44) = "1191104104677b95b000".

Framed-IP-Address(8) = 355206049.

hw_Connect_ID(26) = 22753280.

hw_Product_ID(255) = "H3C SR6602-X".

hw_IP_Host_Addr(60) = "21.44.3.161 00:00:00:00:00:00".

hw_Nas_Startup_Timetamp(59) = 1519641569.

hw_User_Notify(61) = "..O2JeExZUNiB5TkxtKwZ7KSkILQ4=".

通过查看EIA的radius code =1 认证请求报文可发现，该报文中携带的终端mac地址为空，导致EIA和终端类型中记录的终端信息无法进行匹配，从而无法确认该终端的操作系统是否为xp，终端类型无法确认，从而以缺省策略进行认证。

解决方法

因设备侧携带的终端mac地址为空，EIA查询终端表项时，无法使用mac地址进行匹配，导致终端类型匹配识别，无法识别操作系统类型，则以缺省策略进行上线。需联系设备侧确认mac地址为空的具体原因。