iMC EAD组件配置可控软件组检查中文名称的应用不生效问题

EAD解决方案 程晓晨 2019-10-24 发表

组网及说明

无

问题描述

现场使用EAD组件配置了PC可控软件组，设置黑名单应用“迅雷”，根据软件名称进行检查，在操作系统的控制面板中可以看到该软件名称就是“迅雷”。实际测试发现inode安全检查可以正常通过，根据配置来说安全检查应该不通过。

过程分析

1、根据官网EAD配置案例集中可控软件组的配置（http://www.h3c.com/cn/Service/Document_Software/Document_Center/IP_Management/H3C_intelligentize/H3C_intelligentize/Configure/Typical_Configuration_Example/iMC_EAD_Typical_CE-5PW101/）确认现场配置正确，具体需要确认PC可控软件组配置的应用名称与操作系统控制面板-程序中显示的名称一致、可控软件组策略是否被调用在了接入策略中。

2、确认现场策略代理服务器开启，9019端口在网络中放通（注意杀毒软件和防火墙是否开启，是否有中间安全设备阻断）。

图一

3、收集Policysever进程的debug级别日志进行分析发现策略代理服务器下发给iNode的可控软件黑白名单列表为“？？？”乱码无法识别。 收集inode客户端的详细级别日志，分析iNodeSecPKt日志发现iNode收到策略代理服务器发过来的的可控软件黑白名单列表也为“？？？”乱码无法识别。于是怀疑现场iMC服务器操作系统的语言设置问题导致EAD策略代理服务器下发可控软件组黑白名单中中文应用名称为乱码。

Policyserver:

2019-09-18 10:42:29 [INFO] [MsgSender-49] [EadMsgEncoder::encode]null ; EAD????????(2) ; ZrOZvPFz ; null ; 172.16.200.54 ; ?????????

MsgId: 27055

MsgType: 2

attr:ipType: 0

Address: 172.16.200.54

Proxy IP: 172.16.100.13

attr:encrypt: true

attr:compressed: true

strategyMode: autoAdapt

userMessage:

antiIPchange: false

antiAgent: false

antiProxy: false

antiDualNetcard: false

ipSetMode: unlimit

macCheck: false

sameMacCheck: false

antiMultiOS: false

antiMultiip: false

antiVMWareNATservice: false

antiVMWareUSBservice: false

iSupVMCheck: false

iSetWanControl: false

iSetPingOfflineMon: false

damProxyIp: 2886755341

damProxyPort: 9029

heartBeatInterval: 720

heartBeatOutTimes: 3

checkList:
whiteSoftGroup: { ????;???;;;;or;????;office 365 ?????-zh-cn;;;;or;????;VNC Enterprise Edition E4.5.1;;;;or;????;office outlook professional plus 2010;;;;or;????;winrar;;;;or }
blackSoftGroup: {
????;??;;;;or;????;????;;;;or;????;??????;;;;or;????;????;;;;or;????;??;;;;or;????;????;;;;or;????;360????;;;;or }
ifMonitorPassword: false
ifSetLocalPwdPolicy: false
LocalPwdPolicyList:
MinimumPassWordAge=0;MaximumPasswordAge=30;MinimumPasswordLength=0;PasswordComplexity=0;PasswordHistorySize=0;

iNodeSecPkt：
[2019-09-18 10:42:26] [DtlCmn] [2db4] SecPkt sndSecMsg: transfer [2] [27055]
<data>
autoAdapt

false
false
false
false
unlimit
false
false
false
false
false
false
false
false
false
2886755341
9029
720
3

????;???;;;;or
????;office 365 ?????-zh-cn;;;;or
????;VNC Enterprise Edition E4.5.1;;;;or
????;office outlook professional plus 2010;;;;or
????;winrar;;;;or
????;??;;;;or
????;????;;;;or
????;??????;;;;or
????;????;;;;or
????;??;;;;or
????;????;;;;or
????;360????;;;;or
false
false

解决方法

根据如下案例排查并修改iMC所在服务器操作系统语言设置问题后解决。
https://zhiliao.h3c.com/Theme/details/7866