某局点iMC EIA/iNode 认证成功后短时间内掉线并提示安全认证失败“未收到服务器回应，即将强制下线”

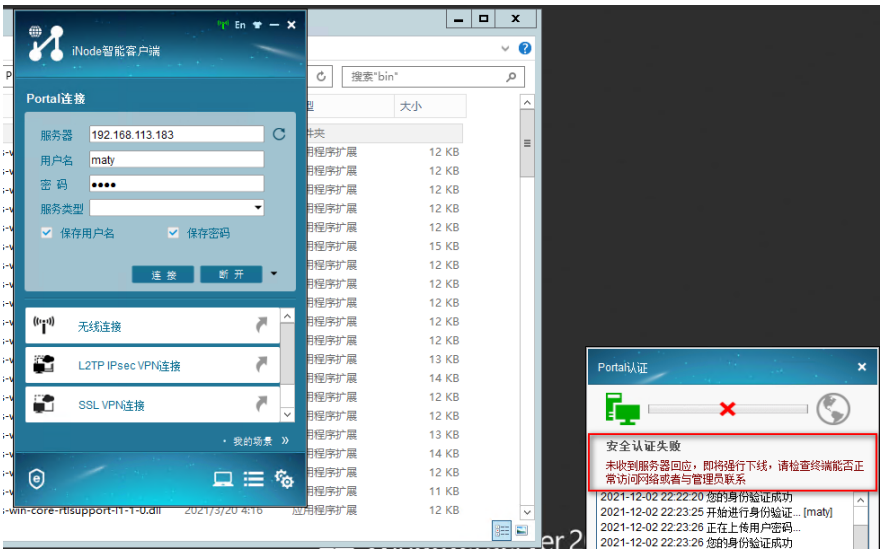
iNode iMC 栗鹏 2021-12-03 发表

组网及说明

8021.1x、portal认证组网都可能出现。

问题描述

iNode认证成功后，短时间内会出现掉线，iNode客户端提示安全认证失败，“未收到服务器回应，即将强制下线，请检查终端能否正常访问网络或者与管理员联系”



过程分析

认证逻辑：

iNode在定制了定制了EAD功能后，在认证成功后，iNode会与iMC EIA策略服务器进行安全检查报文交互。

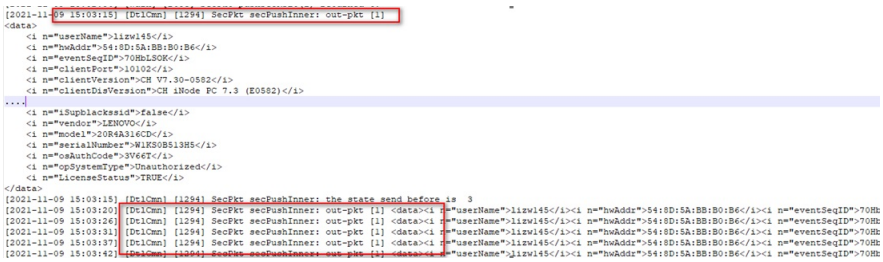
即使没有配置任何安全检查项或者安全策略，也是要正常交互安全检查报文。iNode发起安全检查请求，策略服务器响应结果“不需要检查”。

排查思路：

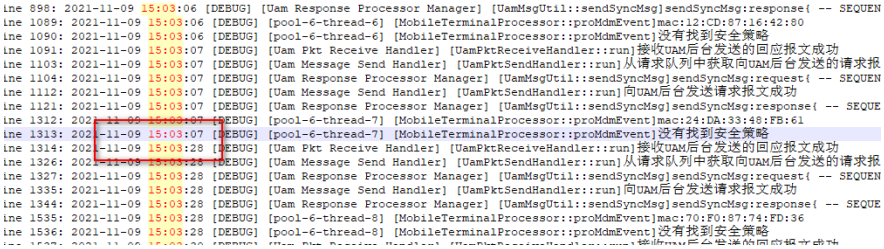
（1）收集iNode详细级别日志、policy server的debug级别日志，客户端与iMC两侧抓包。

（2）分析iNode日志与策略服务器日志；

分析iNode日志（iNodeSecPkt.xxxxxx），记录已经发起了安全认证请求，但是没有收到服务器的回应。

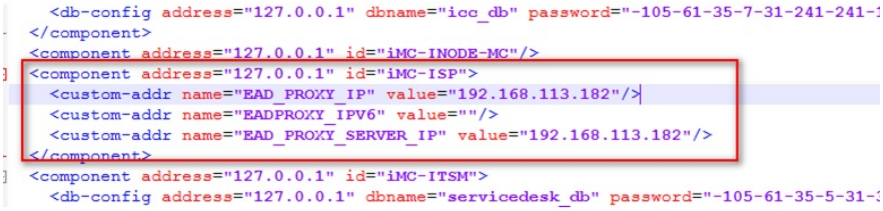


分析策略服务器日志（policyserver），策略服务器并没有收到请求报文。

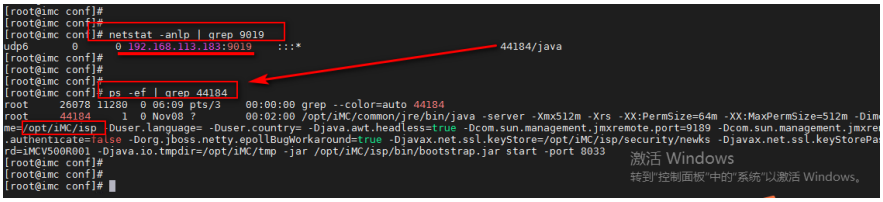


（3）分析抓包文件，过滤udp.port==9019端口查看，目的端口不可达。进一步排查iMC侧进程情况。

（4）检查下iMC策略服务器配置的IP检查iMC/common/conf/server_addr.xml文件，策略服务器的IP是否是iMC 正确的IP地址，如果地址不正确，请修改为正确的IP地址并重启对应的进程生效。



（5）检查policy server、ispserver进程是否正常运行？以及9019端口是否正常被监听？如图所示，正常情况，监听udp 9019端口进程是IP地址为192.168.113.183的java进程，该java进程对应iMC监控代理中ispserver（策略代理服务器）



（6）如果进程监听都正常，则进一步排查网络情况是否存在丢包、防火墙拦截等情况。