

知 iMC部署监控代理部分进程被360天擎主动防御结束进程的问题分析

PLAT 唐斌 2019-06-11 发表

组网及说明

无

问题描述

问题现象：表现为突然发现认证业务不成功，iMC页面访问失败。查看iMC部署监控代理进程标签页，uam、uammon、imcwlndm等大部分后台进程不显示。只有少量iMC进程。

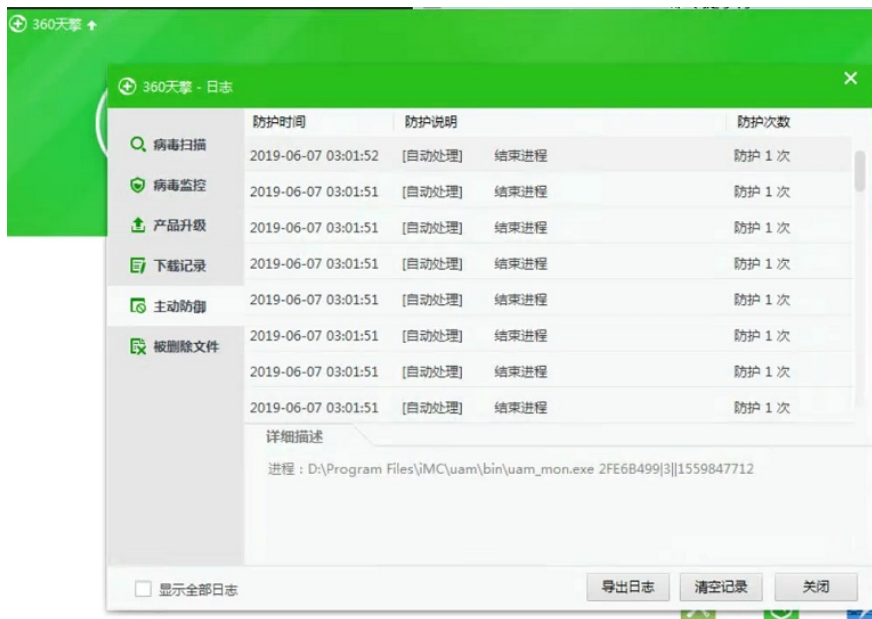
过程分析

查看前台日志，发现凌晨3点左右有错误信息：

ConnectionsNotReadyException[50002]网络连接失败或通信错误

```
2019-06-04 03:02:12 [ERROR] [pool-11-thread-1] [com.imc.fault.browser.func.FaultBoardMgrImpl$4::run]
com.imc.common.ex.GenericApplicationException: com.imf.ConnectionIsNotReadyException[50002] 网络连接失败或通信错误。
    at com.imc.common.ex.GenericApplicationException.newNetworkCommunicateException(GenericApplicationException.java:87)
    at com.imc.common.ExceptionAdvisor.errorAdvise(ExceptionAdvisor.java:75)
    at com.imc.common.HsgComm.sendSyncHsg(HsgComm.java:321)
    at com.imc.fault.browser.dao.FaultBoardDaoImpl.readFaultSortBoardData(FaultBoardDaoImpl.java:162)
    at com.imc.fault.browser.func.FaultBoardMgrImpl$4.run(FaultBoardMgrImpl.java:549)
    at java.util.concurrent.Executors$RunnableAdapter.call(Executors.java:471)
    at java.util.concurrent.FutureTask.runAndReset(FutureTask.java:304)
    at java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.access$301(ScheduledThreadPoolExecutor.java:178)
    at java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run(ScheduledThreadPoolExecutor.java:293)
    at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)
    at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)
    at java.lang.Thread.run(Thread.java:745)
Caused by: com.imf.ConnectionIsNotReadyException
    at com.imf.IMFConnection.write(IMFConnection.java:530)
    at com.imf.AbstractMessageFuture.done(AbstractMessageFuture.java:464)
    at com.imf.MessageWriter.call(MessageWriter.java:83)
    at com.imf.MessageWriter.call(MessageWriter.java:1)
    at com.imf.common.ExecutionService$Execution.execute(ExecutionService.java:410)
    at com.imf.common.ExecutionService$Execution.run(ExecutionService.java:388)
    ... 1 more
```

观察现场环境中存在360天擎，查看发现在凌晨3点左右有主动防御，结束进程的记录。分析问题原因为360天擎版本误杀iMC进程。



解决方法

- 1、卸载天擎软件，重启iMC进程。
- 2、安全软件服务器侧将iMC放入白名单，下发更新安全策略。