**病毒处理简易说明**

1. 根据异常进程的pid查找出和该进程相关的所有文件和网络通信

# top | grep yarn （yarn中毒情况下）

# lsof -p ${pid}

确认相关文件与业务运行无关的全部删除

确认与业务无关的网络通信对端域名或IP，外网访问做禁止操作

1. 查找启动异常进程的用户相关的定时任务

#crontab -l -u ${user}

与业务无关的定时任务脚本及脚本调用的文件或资源，确认与业务无关的全部删除

确认与业务运行无关的定时任务全部删除

1. 按照业务需要开通防火墙规则，不需要的端口和访问全部禁止，kill异常进程重启服务器

下列操作在贵司设备上并未发现异常，如有需要可以检查下：

1. 查看异常前后系统登录验证log
2. 系统开机加载的进程或者脚本