寻找进程被谁kill方法

# 问题背景与现象：

在某环境出现DataNode异常重启，且确认此时未从页面做重启DataNode的操作，需要定位是什么进程kill DataNode 服务端进程。

1. 排查DataNode运行日志和NodeAgent日志，是先收到“RECEIVED SIGNAL 15”再健康检查失败。即先于2016-12-06 11:04:48被kill（或者kill -15），然后实例健康检查才发现异常，重试20次后，于2016-12-06 11:06:52拉起。

2016-12-06 11:04：48,433 | ERROR | SIGTERM handler | RECEIVED SIGNAL 15: SIGTERM | LogAdapter.java:69

2016-12-06 11:04:48,436 | INFO  | Thread-1 | SHUTDOWN\_MSG:

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

SHUTDOWN\_MSG: Shutting down DataNode at 189-39-235-85/189.39.235.85

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/ | LogAdapter.java:45

2016-12-06 11:06:52,744 | INFO  | main | STARTUP\_MSG:

2. 以上日志说明，DataNode先被其他进程杀死，然后健康检查失败，2分钟后，被nodeagent拉起DataNode 进程。

# 定位方法：

打开操作系统审计日志，给审计日志增加记录kill命令的规则，即可定位是何进程发送的kill命令。

## 操作影响

1. 打印审计日志，会消耗一定操作系统性能，经过分析仅影响不到1%

2. 打印审计日志，会占用一定磁盘空间。该日志打印量不大，MB级别，且默认配置有老化机制和检测磁盘剩余空间机制，不会占满磁盘。

## 定位方法

在DataNode进程可能发生重启的所有节点，分别执行以下操作。

1. root用户登录节点，执行service auditd status 命令，确认该服务状态。

Checking for service auditd running

如果该服务未启动，执行service auditd restart 命令重启该服务（无影响，耗时不到1秒）

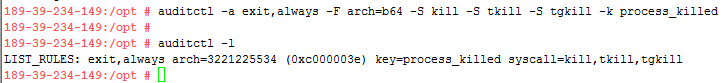
Shutting down auditd done

Starting auditd done

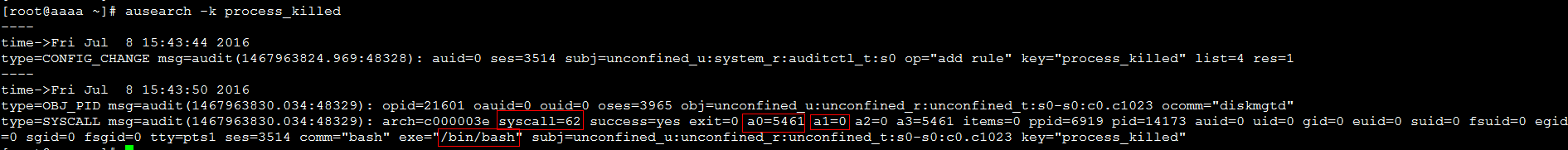
2. 审计日志临时增加 kill命令审计规则

增加规则：auditctl -a exit,always -F arch=b64 -S kill -S tkill -S tgkill -k process\_killed

查看规则：auditctl -l



3. 当进程有异常被kill后，使用 ausearch -k process\_killed 命令，可以查询kill历史。

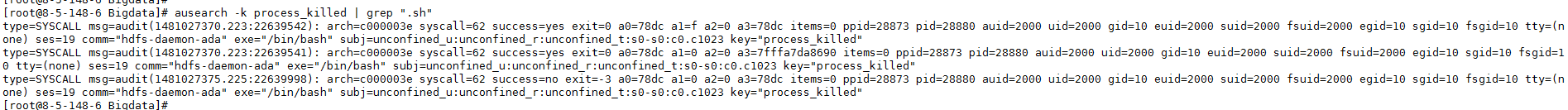


## 验证方法

1. 从页面重启该节点一个实例，如DataNode。

2. 执行ausearch -k process\_killed 命令，确认是否有日志打印。

例如以下命令ausearch -k process\_killed |grep “.sh” ，可以看到是hdfs-daemon-ada\* 脚本，杀的DataNode进程。



## 停止审计kill命令方法

service auditd restart 命令，即会清理临时增加的kill审计日志。

再执行 auditctl –l 命令，如果没有kill相关信息，即说明已清理该规则。