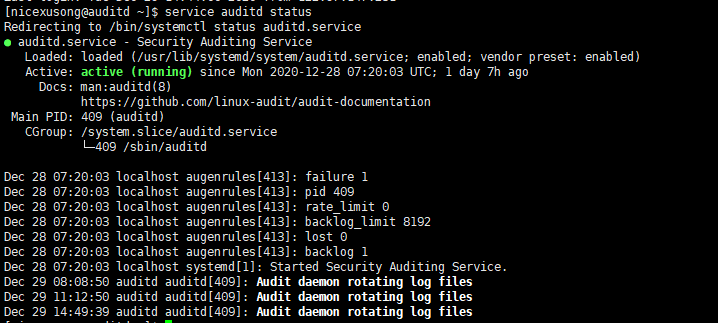
**配置audit审计及cloudlogging查询**

**配置audit审计**

1.首先执行service auditd status，查看auditd服务状态



如果没有开启，执行service auditd start，开启服务

1. 执行auditctl -w /bin/rm -p x -k removefile，监视rm命令操作（临时生效）

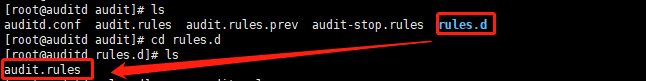


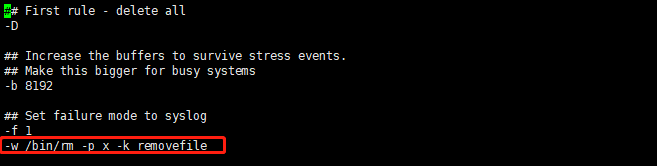
执行auditctl -l，查看生效的规则



1. 编辑/etc/audit/audit.d目录下的audit.rules配置文件，

增加-w /bin/rm -p x -k removefile规则





然后重启audit服务（永久生效）



**安装并配置cloud logging的agent**

4.添加agent的软件包代码库

curl -sSO <https://dl.google.com/cloudagents/add-logging-agent-repo.sh>

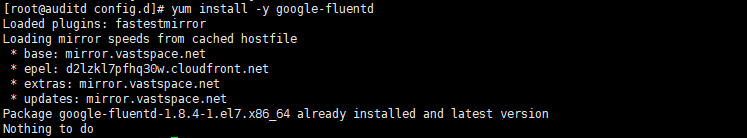
  
bash add-logging-agent-repo.sh



5.安装agent，列出安装可用版本，以选择要安装的版本：

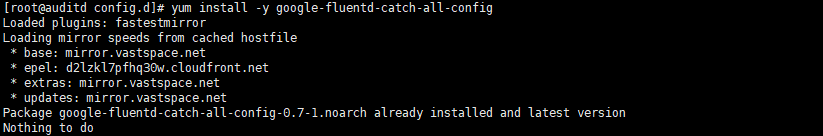
yum list --showduplicates google-fluentd

yum install -y google-fluentd



安装配置文件。

yum install -y google-fluentd-catch-all-config



重启代理服务

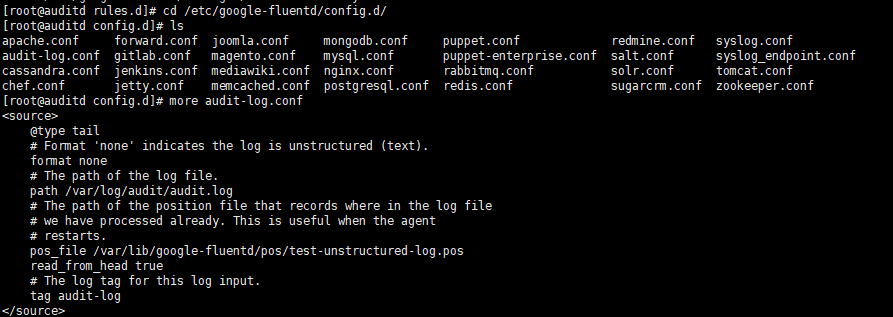
service google-fluentd restart

service google-fluentd status



代理的状态应为 **OK**。

6.创建并配置/etc/google-fluentd/config.d目录下的audit-log.conf 文件，创建后重启service google-fluentd restart服务



<source>

@type tail

# Format 'none' indicates the log is unstructured (text).

format none

# The path of the log file.

path /var/log/audit/audit.log

# The path of the position file that records where in the log file

# we have processed already. This is useful when the agent

# restarts.

pos\_file /var/lib/google-fluentd/pos/test-unstructured-log.pos

read\_from\_head true

# The log tag for this log input.

tag audit-log

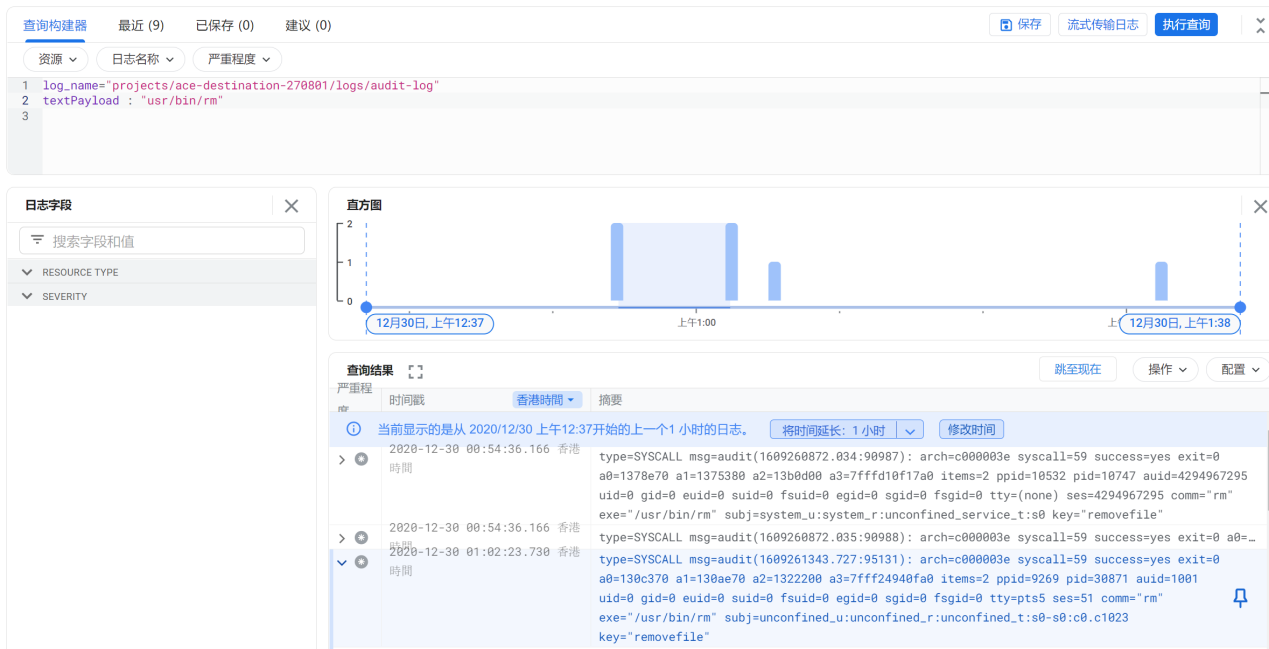
</source>

备注：“path /var/log/audit/audit.log”是linux系统存储audit日志的路径

“tag audit-log”是用于在logging中查询的标签

**使用cloud logging查询**

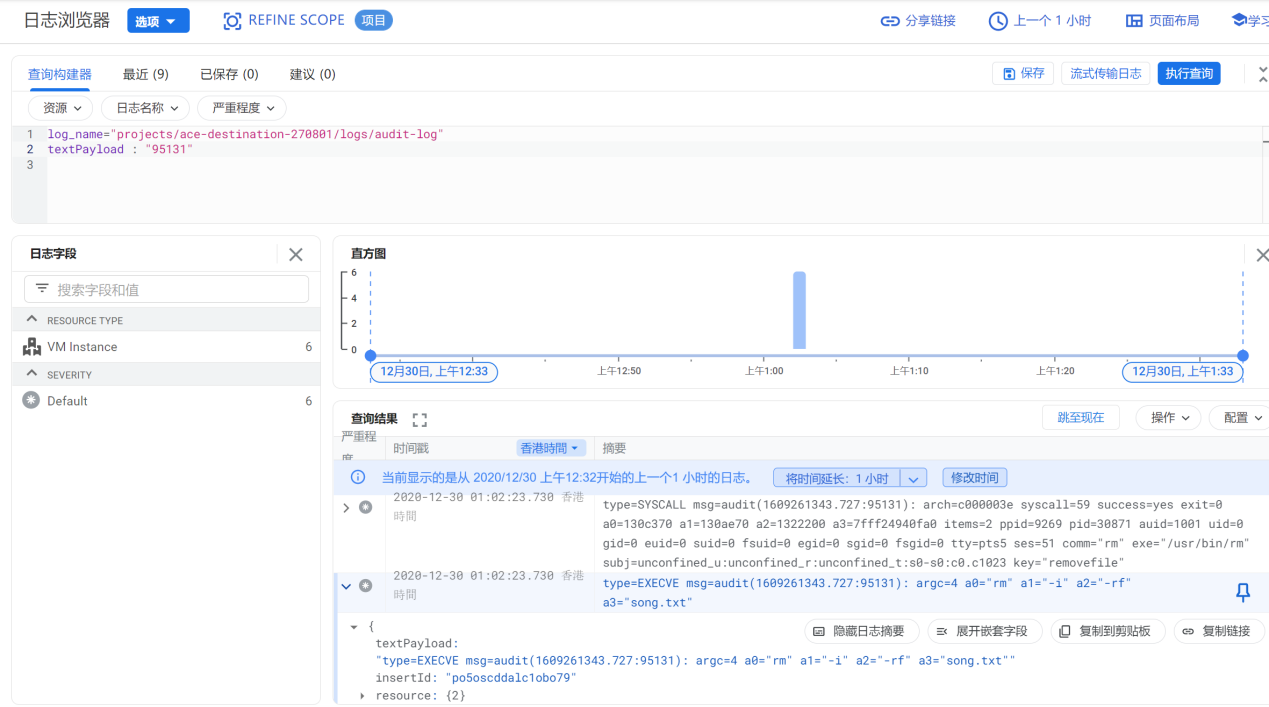
7.查询删除动作，记录下事件ID（事件ID为时间戳“:”后面的数字串，本例为95131）



备注：log\_name="projects/ace-destination-270801/logs/audit-log"

textPayload : "usr/bin/rm"

8.使用上一步中的事件ID来查询被删除的文件，其中，pid表示执行的进程ID，uid表示用户，a3=‘song.txt’表示被删除的文件



备注：log\_name="projects/ace-destination-270801/logs/audit-log"

textPayload : "95131"