原文链接：<https://www.jianshu.com/p/ef0a22cd97ef>

## 准备插件：server\_audit.so

其来源于 mariadb

注意：使用mariadb 与 mysql 对应的版本

MariaDB 5.5 对应 Mysql 5.5

5.5以下的版本都是上述对应关系

MariaDB 10.0 对应 Mysql 5.6

MariaDB 10.1 对应 Mysql 5.7

### 方法一：

MariaDB官网上下载 Linux 的通用版本，解压后/lib/plugin/server\_audit.so

<https://mariadb.org/download/>

### 方法二：

安装 MariaDB 的 docker 环境，

# 查找 MariaDB 的容器ID <MariaDB\_ID>

docker ps

# 进入容器

docker exec –it <MariaDB\_ID> /bin/bash

# 查找 server\_audit.so 所在位置 <path/server\_audit.so>

find / -name server\_audit.so

# 把插件拷贝至宿主机根目录

docker cp <MariaDB\_ID>:/path/server\_audit.so /

## 将插件移动至 mysql 插件目录

# 查找 mysql 插件目录 <mysql\_plugin\_path>

find / -name plugin

# 移动插件至mysql 插件目录

mv /server\_audit.so <mysql\_plugin\_path>

# 设置插件权限

chmod 755 <mysql\_plugin\_path>/server\_audit.so

## 关闭SELinux

# 临时关闭

setenforce 0

# 永久关闭

vi /etc/selinux/config

SELINUX=disabled

如果不关闭，在 mysql 加载插件时会出现 cannot open shared object file: Permission denied 错误

## 设置mysql

# 进入mysql

mysql –u<user> -p<passwd>

# 加载、使用插件

install plugin server\_audit SONAME 'server\_audit.so';

SET GLOBAL server\_audit\_logging=ON;

SET global server\_audit\_events='connect,query';

set global server\_audit\_file\_rotate\_now =on;

为了重新启动后也能生效，可以在 MySQL 的配置文件添加相应的设置。

## 设置 rsyslog

# 查找日志文件路径 <log\_path>

find / -name server\_audit.log

# 配置 rsyslog 文件

vi /etc/rsyslog.conf

#------

input(type="imfile"

File="<log\_path>\*"

Tag="mysql: "

PersistStateInterval="1"

reopenOnTruncate="on"

Severity="info"

Facility="local5"

)

local5.\* @@10.10.100.166:514

#------

# 重启 rsyslog

service rsyslog restart

rsyslog 配置上传 mysql 日志文件时要使用正则匹配，其随着日志文件增大，会出现后加数字的其他文件。

## 附件

server\_audit\_5.5.so 对应 mysql5.5

server\_audit\_5.6.so 对应 mysql5.6