下载地址：

<https://dl.bintray.com/mcafee/mysql-audit-plugin/>

**选择**[audit-plugin-mysql-5.6-1.0.9-541-linux-x86\_64.zip](https://dl.bintray.com/mcafee/mysql-audit-plugin/:audit-plugin-mysql-5.6-1.0.9-541-linux-x86_64.zip)

**将audit插件解压：**

**#unzip audit-plugin-mysql-XXX-**linux-x86\_64.zip

进入解压后的文件目录中的lib目录中，拷贝libaudit\_plugin.so文件到msyql插件目录中：

1、查看mysql插件目录：

mysql> SHOW VARIABLES LIKE 'plugin\_dir'\G

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 1. row \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Variable\_name: plugin\_dir

Value: /usr/local/mysql/lib/plugin/

1. 拷贝libaudit\_plugin.so文件

#cp libaudit\_plugin.so /usr/local/mysql/lib/plugin/

**安装插件:**

方式1、官方推荐，修改my.cnf配置文件，添加plugin-load=AUDIT=libaudit\_plugin.so

方式2、INSTALL PLUGIN AUDIT SONAME 'libaudit\_plugin.so';

开启audit功能 mysql> SET GLOBAL audit\_json\_file=ON;

系统变量：

mysql > show variables like '%audit%';

**设定记录审计日志条件：**

set global audit\_record\_cmds="insert,update,delete,drop,alter" 可设置多个，使用逗号分开。

或者写入配置文件：[mysqld] audit-record-cmds=insert,update,delete,drop,alter

**参数说明：**

audit\_json\_log\_file：json日志文件名，如果audit\_json\_file选项启用，将写审计跟踪到该设置的文件，可以设置为绝对路径

audit\_json\_file：启用或关闭json 日志文件

audit\_json\_file\_sync：json文件同步周期，如果大于0，将每多少次写后同步到磁盘

audit\_json\_file\_flush：将刷新日志文件，关闭和重新打开文件，能手动进行轮转日志

audit\_json\_socket\_name：json unix socket name，如果audit\_json\_socket选项启用，将写审计日志到该unix套接字

audit\_json\_socket：启用或关闭json unix socket

audit\_uninstall\_plugin：在命令行或配置文件启用或关闭AUDIT uninstall 插件

audit\_validate\_checksum：启用或关闭mysqld二进制校验和确认

audit\_checksum：在命令行或配置文件启用mysqld校验和确认，当设置audit\_offsets

audit\_record\_cmds：逗号分隔的标记记录哪些命令到审计日志，如insert、update、delete

audit\_record\_objs：逗号分隔的哪些对象记录到审计日志，格式为database.table，支持通配符

audit\_whitelist\_users：逗号分隔的白名单用户，将不记录到审计日志

audit\_header\_msg：启用或关闭记录消息头，1.0.6引入

audit\_password\_masking\_cmds：逗号分隔的命令，将隐藏密码，如CREATE\_USER,GRANT,SET\_OPTION,SLAVE\_START,CREATE\_SERVER,ALTER\_SERVER,CHANGE\_MASTER，1.0.6引入

audit\_password\_masking\_regex：使用PCRE正则表达式屏蔽密码，仅仅audit\_password\_masking\_cmds指定的命令，1.0.6引入

查看日志，日志在mysql数据目录里面：

#more mysql-audit.json

**日志格式：**

**# more mysql-audit.json**

**{"msg-type":"header","date":"1450148043701","audit-version":"1.0.9-541","audit-protocol-version":"1.0","hostname":"olmaster1.com","mysql-version":"5.6.27-log","mysql-program":"/usr/local/mysql/bin/mysqld","mysql-socket":"/usr/local/mysql/data/mysql.sock","mysql-port":"3306"}**

**{"msg-type":"activity","date":"1450148120021","thread-id":"1","query-id":"16","user":"root","priv\_user":"root","host":"localhost","ip":"","cmd":"show\_variables","objects":[{"db":"information\_schema","name":"/tmp/#sql\_4ef\_0","obj\_type":"VIEW"}],"query":"show variables like '%audit%'"}**

**{"msg-type":"activity","date":"1450148818775","thread-id":"1","query-id":"17","user":"root","priv\_user":"root","host":"localhost","ip":"","cmd":"select","query":"SELECT DATABASE()"}**

**{"msg-type":"activity","date":"1450148818796","thread-id":"1","query-id":"18","user":"root","priv\_user":"root","host":"localhost","ip":"","cmd":"InitDB","objects":[{"db":"newdb","obj\_type":"DATABASE"}],"query":"Init DB"}**

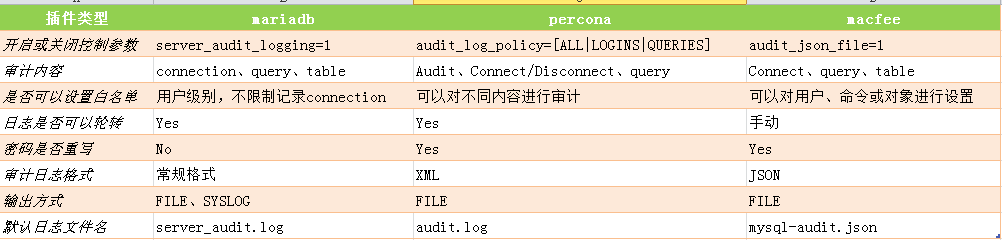
**{"msg-type":"activity","date":"1450148818796","thread-id":"1","query-id":"19","user":"root","priv\_user":"root","host":"localhost","ip":"","cmd":"show\_databases","objects":[{"db":"information\_schema","name":"/tmp/#sql\_4ef\_0","obj\_type":"VIEW"}],"query":"show databases"}**

**{"msg-type":"activity","date":"1450148818810","thread-id":"1","query-id":"20","user":"root","priv\_user":"root","host":"localhost","ip":"","cmd":"show\_tables","objects":[{"db":"information\_schema","name":"/tmp/#sql\_4ef\_0","obj\_type":"VIEW"}],"query":"show tables"}**

**{"msg-type":"activity","date":"1450148821360","thread-id":"1","query-id":"21","user":"root","priv\_user":"root","host":"localhost","ip":"","cmd":"show\_tables","objects":[{"db":"information\_schema","name":"/tmp/#sql\_4ef\_0","obj\_type":"VIEW"}],"query":"show tables"}**

**{"msg-type":"activity","date":"1450148840537","thread-id":"1","query-id":"23","user":"root","priv\_user":"root","host":"localhost","ip":"","cmd":"create\_table","objects":[{"db":"newdb","name":"tb1","obj\_type":"TABLE"}],"query":"create table tb1(id int)"}**

**常见审计插件对比：**



备注：mysql官方审计插件目前只有企业版提供此功能，社区版不提供。并且官方插件的功能相对较弱。