# **[MySQL审计管理](http://www.linuxe.cn/post-557.html)**

### **MariaDB server\_audit 审计插件**

|  |  |
| --- | --- |
| wget https://downloads.mariadb.com/MariaDB/mariadb-10.5.9/bintar-linux-x86\_64/mariadb-10.5.9-linux-x86\_64.tar.gz  tar xf mariadb-10.5.9-linux-x86\_64.tar.gz  cd mariadb-10.5.9-linux-x86\_64/lib/plugin/  cp -a server\_audit.so /data/mysql/lib/plugin/  cd /data/mysql/lib/plugin/  chown mysql.mysql server\_audit.so  cd /data/mysql/data  tf server\_audit.log  **#写入/etc/my.cnf 前要先创建日志目录。**  **mkdir -p /var/log/mysql**  **chown -R mysql:mysql /var/log/mysql**  >INSTALL PLUGIN server\_audit SONAME 'server\_audit.so';  >show variables like '%server\_audit%';   |  | | --- | | set global server\_audit\_logging=on;  set gLOBAL server\_audit\_file\_rotate\_size=1073741824;#1G大小  set global server\_audit\_file\_rotations=10;  set global server\_audit\_file\_path='/var/log/mysql/';  set global server\_audit\_events='CONNECT,TABLE,QUERY\_DDL,QUERY\_DCL,QUERY\_DML\_NO\_SELECT'; |   [mysqld]  方式一  log\_output=FILE  server\_audit\_file\_path=/var/log/mysql/audit.log  server\_audit\_events = 'QUERY\_DCL,QUERY\_DML\_NO\_SELECT,QUERY\_DML,QUERY\_DDL,TABLE,QUERY,CONNECT'  server\_audit\_logging=1  方式二 **暂时采用这种**  server\_audit\_logging=ON  server\_audit\_file\_path=/var/log/mysql/audit.log  server\_audit=FORCE\_PLUS\_PERMANENT # 防止审计插件被卸载  server\_audit\_file\_rotate\_size=500M  server\_audit\_file\_rotations=10  方式三  在参数文件my.cnf里面修改一些系统变量参数。如下所示  要先建mysql\_audit目录    #############################MariaDB Audit Plugin####################################  plugin\_load\_add=server\_audit  server\_audit\_logging=1  server\_audit\_events=CONNECT,TABLE,QUERY\_DDL,QUERY\_DCL,QUERY\_DML\_NO\_SELECT  server\_audit\_file\_path=/var/log/mysql/audit.log'  server\_audit\_file\_rotate\_size=500M  server\_audit\_file\_rotations=10 |

<https://blog.51cto.com/wujianwei/2647872>

<https://zhuanlan.zhihu.com/p/67608184>

<https://blog.51cto.com/u_15127638/2749669>

[IMG_256](https://www.cnblogs.com/waynechou/p/javascript:void(0);)

server\_audit\_output\_type：指定日志输出类型，可为SYSLOG或FILE

server\_audit\_logging：启动或关闭审计

server\_audit\_events：指定记录事件的类型，可以用逗号分隔的多个值(connect,query,table)，如果开启了查询缓存(query cache)，查询直接从查询缓存返回数据，将没有table记录

server\_audit\_file\_path：如server\_audit\_output\_type为FILE，使用该变量设置存储日志的文件，可以指定目录，默认存放在数据目录的server\_audit.log文件中

server\_audit\_file\_rotate\_size：限制日志文件的大小

server\_audit\_file\_rotations：指定日志文件的数量，如果为0日志将从不轮转

server\_audit\_file\_rotate\_now：强制日志文件轮转

server\_audit\_incl\_users：指定哪些用户的活动将记录，connect将不受此变量影响，该变量比server\_audit\_excl\_users优先级高

server\_audit\_syslog\_facility：默认为LOG\_USER，指定facility

server\_audit\_syslog\_ident：设置ident，作为每个syslog记录的一部分

server\_audit\_syslog\_info：指定的info字符串将添加到syslog记录

server\_audit\_syslog\_priority：定义记录日志的syslogd priority

server\_audit\_excl\_users：该列表的用户行为将不记录，connect将不受该设置影响

server\_audit\_mode：标识版本，用于开发测试

**卸载 server\_audit**

mysql> UNINSTALL PLUGIN server\_audit;

mysql> show variables like '%audit%';

Empty set (**0.00** sec)