# percona 5.7审计功能

Percona审计日志插件提供了数据库执行的连接和查询活动的监控记录，每一个事件都有一个NAME字段和唯一的RECORD\_ID和 TIMESTAMP字段。

一、开启审计功能

安装审计插件可以通过添加配置文件重启数据库加载，也可以动态安装。

# 配置文件加载

[mysqld]

plugin-load=audit\_log.so

# 加载插件列表

mysql> INSTALL PLUGIN audit\_log SONAME 'audit\_log.so';

二、参数介绍

jianwei.zheng@localhost : (none) 16:30:53>show variables like '%audit%';

+-----------------------------+----------------------------+

| Variable\_name | Value |

+-----------------------------+----------------------------+

| audit\_log\_buffer\_size | 1048576 |

| audit\_log\_exclude\_accounts | 'cactiuser'@'%' |

| audit\_log\_exclude\_commands | |

| audit\_log\_exclude\_databases | |

| audit\_log\_file | /data/logs/mysql/audit.log |

| audit\_log\_flush | OFF |

| audit\_log\_format | JSON |

| audit\_log\_handler | FILE |

| audit\_log\_include\_accounts | |

| audit\_log\_include\_commands | |

| audit\_log\_include\_databases | |

| audit\_log\_policy | LOGINS |

| audit\_log\_rotate\_on\_size | 536870912 |

| audit\_log\_rotations | 10 |

| audit\_log\_strategy | ASYNCHRONOUS |

| audit\_log\_syslog\_facility | LOG\_USER |

| audit\_log\_syslog\_ident | percona-audit |

| audit\_log\_syslog\_priority | LOG\_INFO |

+-----------------------------+----------------------------+

1.audit\_log\_buffer\_size：审计缓存，建议设置为4096的倍数，该参数只有在audit\_log\_strategy为ASYNCHRONOUS时生效。

2.audit\_log\_exclude\_accounts：排除审计用户；可动态设置。

3.audit\_log\_file：指定审计日志路径及文件名称，路径可为相对路径或绝对路径。

4.audit\_log\_format：日志格式，共有OLD, NEW, JSON, 和 CSV四种格式；不可动态调整。

5.audit\_log\_policy：指定审计日志记录的事件。

ALL - 记录所有事件  
LOGINS - 只记录登录连接信息  
QUERIES - 只记录查询事件  
NONE - 不记录任何事件

6.audit\_log\_rotate\_on\_size：指定最大审核日志大小。

7.audit\_log\_rotations：指定保存审核日志个数。

8.audit\_log\_strategy：指定审计日志的刷新策略，只有在 audit\_log\_handler 为 'FILE'时该变量才生效。

ASYNCHRONOUS - 异步(默认)，使用内存缓冲区，缓冲区满时不删除消息  
PERFORMANCE - 使用内存缓冲区，缓冲区满时删除消息  
SEMISYNCHRONOUS - 直接写入到文件中，通过操作系统刷新同步事件  
SYNCHRONOUS - 直接写入到文件中，实时同步刷新事件

9.audit\_log\_handler：指定审核日志保存格式：FILE、SYSLOG。

三、配置文件需要添加如下内容：

#audit

plugin-load = audit\_log.so

audit\_log\_rotate\_on\_size = 512M

audit\_log\_rotations = 10

audit\_log\_policy = LOGINS

audit\_log\_format = JSON

audit\_log\_file = /data/logs/mysql/audit.log

audit\_log\_handler = FILE

audit\_log\_exclude\_accounts = cactiuser@%

四、参考：<https://www.percona.com/doc/percona-server/5.7/management/audit_log_plugin.html>