

Mysql Audit 安装 步骤

环境

1. Mysql 版本 5.6 及以上 版本 支持 Audit 插件 安装
2. 操作系统
 1. Mysql 5.6 及以上 版本 , Mysql 社区版 Enterprise Edition 版本 支持 安装
 2. MariaDB 10.5 及以上 版本 Audit Plugin 插件 MariaDB 10.5 及以上 版本 支持 Audit 插件 安装

安装步骤

1. Mysql 安装 插件 目录 查看

```
mysql> show global variables like 'plugin_dir';
+-----+-----+
| Variable_name | Value                |
+-----+-----+
| plugin_dir    | //usr/local/mysql/lib/plugin/ |
+-----+-----+
1 row in set (0.00 sec)
```

- 插件 目录 查看 结果 显示 //usr/local/mysql/lib/plugin/ 目录 存在

2. audit 插件 安装

```
$> cp server_audit.so /usr/local/mysql/lib/plugin/
```

3. Mysql 安装 Audit 插件 步骤

```
mysql> install plugin server_audit soname 'server_audit.so';
Query OK, 0 rows affected (0.00 sec)
mysql> show plugins;
```

+-----+-----+-----+-----+-----+				
Name	Status	Type	Library	License
+-----+-----+-----+-----+-----+				
binlog	ACTIVE	STORAGE ENGINE	NULL	GPL
mysql_native_password	ACTIVE	AUTHENTICATION	NULL	GPL
sha256_password	ACTIVE	AUTHENTICATION	NULL	GPL
CSV	ACTIVE	STORAGE ENGINE	NULL	GPL
MyISAM	ACTIVE	STORAGE ENGINE	NULL	GPL
MRG_MYISAM	ACTIVE	STORAGE ENGINE	NULL	GPL
PERFORMANCE_SCHEMA	ACTIVE	STORAGE ENGINE	NULL	GPL
MEMORY	ACTIVE	STORAGE ENGINE	NULL	GPL
InnoDB	ACTIVE	STORAGE ENGINE	NULL	GPL
INNODB_TRX	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_LOCKS	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_LOCK_WAITS	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_CMP	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_CMP_RESET	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_CMPMEM	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_CMPMEM_RESET	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_CMP_PER_INDEX	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_CMP_PER_INDEX_RESET	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_BUFFER_PAGE	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_BUFFER_PAGE_LRU	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_BUFFER_POOL_STATS	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_TEMP_TABLE_INFO	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_METRICS	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_FT_DEFAULT_STOPWORD	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_FT_DELETED	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_FT_BEING_DELETED	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_FT_CONFIG	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_FT_INDEX_CACHE	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_FT_INDEX_TABLE	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_SYS_TABLES	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_SYS_TABLESTATS	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_SYS_INDEXES	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_SYS_COLUMNS	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_SYS_FIELDS	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_SYS_FOREIGN	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_SYS_FOREIGN_COLS	ACTIVE	INFORMATION SCHEMA	NULL	GPL

INNODB_SYS_TABLESPACES	ACTIVE	INFORMATION SCHEMA	NULL	GPL	
INNODB_SYS_DATAFILES	ACTIVE	INFORMATION SCHEMA	NULL	GPL	
INNODB_SYS_VIRTUAL	ACTIVE	INFORMATION SCHEMA	NULL	GPL	
partition	ACTIVE	STORAGE ENGINE	NULL	GPL	
ARCHIVE	ACTIVE	STORAGE ENGINE	NULL	GPL	
FEDERATED	DISABLED	STORAGE ENGINE	NULL	GPL	
BLACKHOLE	ACTIVE	STORAGE ENGINE	NULL	GPL	
ngram	ACTIVE	FTPARSER	NULL	GPL	
validate_password	ACTIVE	VALIDATE PASSWORD	validate_password.so	GPL	
SERVER_AUDIT	ACTIVE	AUDIT	server_audit.so	GPL	
+-----+-----+-----+-----+-----+					

4. audit `TABLES` `TABLES` `TABLES` `SERVER_AUDIT` `TABLES` `TABLES` `TABLES`

5. Audit `TABLES` `TABLES` `TABLES` 1. `TABLES` `TABLES`

```
mysql> set global server_audit_events=connect;
Query OK, 0 rows affected (0.00 sec)
```

1. `TABLES` `TABLES` `TABLES`

```
mysql> set global server_audit_file_path='//usr/local/mysql/logs/server_audit.log';
Query OK, 0 rows affected (0.00 sec)
```

2. `TABLES` `TABLES` `TABLES`

```
mysql> set global server_audit_file_rotate_now=1;
Query OK, 0 rows affected (0.00 sec)
```

3. `TABLES` `TABLES` `TABLES` `TABLES` , 10M `TABLES` (Format : Byte)

```
mysql> set global server_audit_query_log_limit=10240000;
```

6. `TABLES` `TABLES`

```
mysql> set global server_audit_file_rotations=10;
Query OK, 0 rows affected (0.00 sec)
```

- 10 `TABLES` `TABLES` (`TABLES` `TABLES` `TABLES` `TABLES` `TABLES` `TABLES`)

7. Audit `TABLES`

```
mysql> set global server_audit_logging=1;
Query OK, 0 rows affected (0.00 sec)
```

8.  

```
mysql> show global variables like '%audit%';
```

Variable_name	Value
server_audit_events	CONNECT
server_audit_excl_users	
server_audit_file_path	//usr/local/mysql/logs/server_audit.log

|
| server_audit_file_rotate_now | ON

|
| server_audit_file_rotate_size | 1000000

|
| server_audit_file_rotations | 10

|
| server_audit_incl_users |

|
| server_audit_loc_info | 0000 |
| server_audit_logging | ON

| server_audit_mode | 1

| server_audit_output_type | file

| server_audit_query_log_limit | 10240000

| server_audit_syslog_facility | LOG_USER

| server_audit_syslog_ident | mysql-server_auditing

16 rows in set (0.01 sec)

9. $\square \square$ $\square \square$ $\square \square$ $\square \square$

```
$> ls -l //usr/local/mysql/logs/server_audit.log
-rw-r----- 1 stoauser stoauser 81 Apr 24 17:01 /usr/local/mysql/logs/server_audit.log

$> tail -f //usr/local/mysql/logs/server_audit.log
20190424 17:01:06,DB-TEST,root,localhost,7,0,DISCONNECT,,,0
20190424 17:01:35,DB-TEST,root,localhost,8,0,CONNECT,,,0
20190424 17:01:46,DB-TEST,root,localhost,8,0,DISCONNECT,,,0
```

10.    

```
$> vi /etc/my.cnf
...
```

```
##### Audit #####
plugin_load_add          = server_audit
server_audit_logging     = on
server_audit_events      = connect
server_audit_output_type = file
server_audit_file_path   = /usr/local/mysql/logs/server_audit.log
server_audit_file_rotate_now = ON
server_audit_file_rotate_size = 1000000
server_audit_file_rotations = 1024
...
```



1. Log output ☐ syslog ☐ ☐ ☐ server_audit_output_type ☐ syslog ☐ ☐ .
2. File ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

Reference

- <https://mariadb.com/kb/en/library/mariadb-audit-plugin-log-settings/>

- <https://dba.stackexchange.com/questions/178213/mysql-audit-and-general-log>
 - <https://mariadb.com/kb/en/library/mariadb-audit-plugin/>
-

Revision #1

Created 6 June 2022 16:12:24 by artop0420

Updated 8 June 2022 04:00:15 by artop0420