

# Mysql Audit 기능 설정

## 개 요

1. Mysql내에 접근기록을 사용할 수 있는 Audit 플러그인 설명
2. 제약사항
  1. Mysql 5.6이상 설치가 가능하나, Mysql내에는 Enterprise Edition만 제공되는 것으로 파악
  2. MariaDB내에는 Audit Plugin이 제공되어 MariaDB에 저장된 플러그인을 통해 Audit 기능 활성화 가능

## 설치 방법

1. Mysql 접속 후 플러그인 경로 확인

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

- 이경우 플러그인이 저장된 경로는 //usr/local/mysql/lib/plugin/ 경로로 설정되어 있음

2. audit 플러그인 복사

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

3. Mysql에 Audit 플러그인 연동

```
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 플러그인 설치 후 맨 마지막 SERVER\_AUDIT항목이 보이면 설치 완료

5. Audit 관련 설정 진행1. 이벤트 설정

```

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

```

1. 로그 경로 설정

```

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

```

2. 로그 로테이트 설정

```

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

```

3. 파일당 최대 사이트 설정, 10M로 설정예시 (Format : Byte)

```

mysql> set global server_audit_query_log_limit=10240000;

```

6. 보관주기 설정

```

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

```

- 10개 보관 설정 (허용된 파일수에 도달하면 오래된 파일을 덮어씀)

7. Audit 기능활성화

```

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

```

8. 설정값 확인

```

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 | OOOO |
| 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

| server_audit_syslog_info |

| server_audit_syslog_priority | LOG_INFO

+-----+
16 rows in set (0.01 sec)

```

## 9. 로그 생성 여부 확인

```

$> 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. 영구적용을 위해 설정값 적용

```

$> 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
...

```

# 기타사항

1. Log output 을 syslog로 전달이 가능하며 server\_audit\_output\_type 값을 syslog로 변경하면 된다.
2. File 방식으로 사용할 경우 생성되는 로그는 격리된 공간에서 저장하는 것을 추천

#### 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