Original Title: Auditing für MySQL – Aber wie?

DOAG Conference 2013

Nürnberg

Who am I?

- Ralf Gebhardt
- Principal Sales Engineer @ SkySQL
- Joined MySQL GmbH in 2002
- Worked for MySQL@Sun and MySQL@Oracle until June 2011

Now we are one company

Agenda

- Why Auditing?
- Auditing without Audit Plugin
- Audit Plugins for MySQL / MariaDB
- Audit Plugin
  - Installation
  - Configuration
  - The Audit Log
  - Monitoring

Why Auditing?

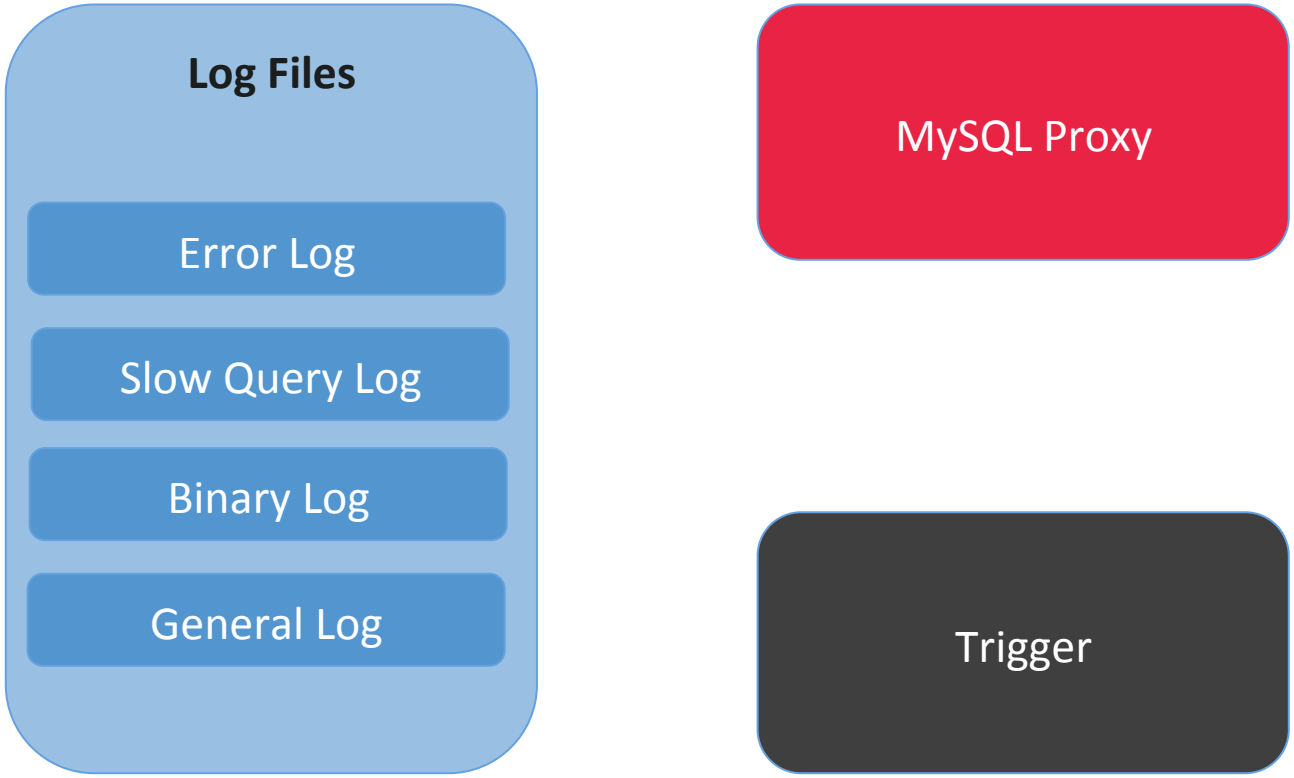
- Monitoring System Access
- Locating Errors
- Discovering Frauds
- Improvement of Internal Control
- Proving the fulfillment of security standards
- And more

What to Monitor

- CONNECTION
  - CONNECT
  - DISCONNECT
  - FAILED CONNECT
- QUERY
  - DDL
  - DML+TCL
  - DCL
- OBJECT
  - DATABASE
  - TABLES

TIMESTAMP
HOST
USER
(SESSION)

Auditing without Audit Plugin



Auditing without Audit Plugin

- Error log
  - Only failed connects can be logged. `log_warnings` system variable needs to be set
  - No queries
- Slow query log
  - Could log everything if `long_query_time` set to 0
  - Connections and failed requests are missing
  - Format of the log file not easy to parse

Auditing without Audit Plugin

- Binary Log
  - Only includes queries that modify data
- General Log
  - Includes connects, failed connects, queries
  - No filtering
  - Format of the log file difficult to parse

Auditing without Audit Plugin

- Triggers
  - Do not exist for SELECT and CONNECT
  - Only per table, painful to maintain
- MySQL Proxy
  - Could be used, custom scripts need to be created
  - Did not reach GA status yet

The MySQL/MariaDB Plugin Architecture

- Plugin Architecture is a major differentiator of MySQL and MariaDB
- Plugins for
  - Storage Engines
  - Information Schema
  - Authentication Plugin
  - Audit Plugin
- `SHOW PLUGINS`
- Audit Plugin API since MySQL 5.1

Audit Plugins for MySQL / MariaDB

MySQL Enterprise Audit
Oracle

MySQL-Audit
McAfee

MariaDB Audit Plugin
MariaDB

Community?

MySQL Enterprise Audit

- Commercial
  - Included in MySQL Enterprise Subscription
- Auditing to XML
  - Audit Log Strategies available
- Only top-level-statements are logged
- Variables how to handle log
  - Asynchronous vs. synchronous writes to disk

MySQL-Audit from McAfee

- Open Source
- Offsets to data structure needed
  - audit_offsets=6464, 6512, 4072, 4512, 104, 2584
- Monitor internal statements (from triggers, stored procedures)
- Auditing to
  - File in JSON format
  - Socket
- https://github.com/mcafee/mysql-audit

MariaDB Audit Plugin

- Open Source
  - Support available
- Auditing to
  - File (comma delimited format)
  - Syslog
- Modified Plugin API in MariaDB
  - Audit Plugin compatible with MySQL Server
  - Allows to monitor table level events (MariaDB)

Audit Plugin Installation

- Provided as dynamic Library
  - server_audit.so / server_audit.dll
- Needs to be in the plugin directory
  - SHOW GLOBAL VARIABLES LIKE „plugin_dir“;
- Plugin can be loaded via
  - Startup parameter
  - my.cnf / my.ini
  - SQL command

Audit Plugin Installation

```
SHOW GLOBAL VARIABLES LIKE 'plugin_dir';
+---------------+-------------------------------+
| Variable_name | Value                         |
+---------------+-------------------------------+
| plugin_dir    | /usr/local/mysql/lib/plugin/ |
+---------------+-------------------------------+
```

```
[mysqld]
...
plugin-load=server_audit=server_audit.so
server_audit=FORCE_PLUS_PERMANENT
..
```

```
INSTALL PLUGIN server_audit SONAME 'server_audit.so'
```

Configuration in General

- Configuration possible by using SET commands or my.cnf
  - Load plugin once before you add variables to my.cnf
- For permanent changes use my.cnf
- Use SET to change a variable for testing or to avoid a server restart

MariaDB Audit Plugin Configuration

- Three types of events
  - CONNECT, QUERY, TABLE (only MariaDB +5.5.31)
- Exclude and Include User Lists
  - For QUERY and TABLE events
- Logging to
  - Syslog
    - Some syslog related parameters can be defined
  - File
    - Path and filename, size and rotation

MariaDB Audit Plugin Configuration – Event Types

- CONNECT
  - Connects, disconnects, failed connects
- QUERY
  - Executed queries
  - Error Code will be logged (0 = success)
- TABLE
  - Only supported for MariaDB 5.5.31 or newer versions
  - READ, WRITE, CREATE, ALTER, RENAME, DROP

MariaDB Audit Plugin Configuration Options

```
SHOW GLOBAL VARIABLES like 'server_audit%';
+-------------------------------+-----------------------------------+
| Variable_name                 | Value                             |
+-------------------------------+-----------------------------------+
| server_audit_events           | CONNECT,QUERY,TABLE               |
| server_audit_excl_users       | cms,drupal,batch                  |
| server_audit_file_path        | /usr/local/mysql/data/audittest   |
| server_audit_file_rotate_now  |                                   |
| server_audit_file_rotate_size | 1000000                           |
| server_audit_file_rotations   | 1                                 |
| server_audit_incl_users       |                                   |
| server_audit_logging          | ON                                |
| server_audit_mode             | 1                                 |
| server_audit_output_type      | file                              |
| server_audit_syslog_facility  | LOG_USER                          |
| server_audit_syslog_ident     | mysqlserver_auditing              |
| server_audit_syslog_info      |                                   |
| server_audit_syslog_priority  | LOG_INFO                          |
+-------------------------------+-----------------------------------+
```

MariaDB Audit Plugin
The Audit Log

- Timestamp
- Serverhost
- User
- Host
- Connection-Id
- Query-Id
- Operation
- Active Database
- Object
- Returncode

MariaDB Audit Plugin
The Audit Log Format

- General format for type file

```
[timestamp],[serverhost],[username],[host],[connectionid],[queryid],
[operation],[database],[object],[retcode]
```

- General format for type syslog

```
[timestamp] [syslog_host] [syslog_ident]: [syslog_info] [serverhost],
[username],[host],[connectionid],[queryid],[operation],[database],
[object],[retcode]
```

MariaDB Audit Plugin Examples

- Events of type CONNECT

```
20130810 00:05:30,localhost.localdomain,root,localhost,2,0,CONNECT,db1,,0
20130810 00:05:53,localhost.localdomain,root,localhost,2,0,DISCONNECT,,,0
20130810 00:06:28,localhost.localdomain,unknownuser,localhost,3,0,FAILED_CONNECT,,,1045
20130810 00:06:28,localhost.localdomain,unknownuser,localhost,3,0,DISCONNECT,,,0
```

- Events of type TABLE

```
20130810 02:21:06,localhost.localdomain,John,localhost,3,25,CREATE,db1,services,
20130810 02:21:06,localhost.localdomain,John,localhost,3,27,READ,db1,services,
20130810 02:21:07,localhost.localdomain,John,localhost,3,29,WRITE,db1,services,
20130810 02:21:27,localhost.localdomain,John,localhost,3,35,ALTER,db1,services,
20130810 02:21:27,localhost.localdomain,John,localhost,3,36,RENAME,db1,services|db1.service,
20130810 02:21:45,localhost.localdomain,John,localhost,3,38,DROP,db1,services_new,
```

MariaDB Audit Plugin Examples

- Events of type TABLE, QUERY using Views

```
20130810 02:21:06,localhost.localdomain,John,localhost,3,27,READ,db1,services,
20130810 02:21:06,localhost.localdomain,John,localhost,3,27,READ,db1,services_types,
20130810 02:21:06,localhost.localdomain,John,localhost,3,27,QUERY,db1,'CREATE VIEW db1.myview
AS SELECT * FROM services WHERE typeid IN (SELECT id FROM services_types WHERE
name="consulting")',0
20130810 02:21:07,localhost.localdomain,John,localhost,3,31,READ,db1,services,
20130810 02:21:07,localhost.localdomain,John,localhost,3,31,READ,db1,services_types,
20130810 02:21:07,localhost.localdomain,John,localhost,3,31,QUERY,db1,'SELECT * from myview',0
```

MariaDB Audit Plugin Examples

- Events of type TABLE, QUERY using DROP

```
20130810 02:21:45,localhost.localdomain,John,localhost,3,38,READ,mysql,proc,
20130810 02:21:45,localhost.localdomain,John,localhost,3,38,DROP,db1,services_types,
20130810 02:21:45,localhost.localdomain,John,localhost,3,38,DROP,db1,services_new,
20130810 02:21:45,localhost.localdomain,John,localhost,3,38,DROP,db1,myview,
20130810 02:21:45,localhost.localdomain,John,localhost,3,38,WRITE,mysql,proc,
20130810 02:21:45,localhost.localdomain,John,localhost,3,38,WRITE,mysql,event,
20130810 02:21:45,localhost.localdomain,John,localhost,3,38,QUERY,db1,'drop database db1',0
```

Monitoring MariaDB Audit Plugin

- The status of the MariaDB Audit Plugin can be established by the standard `SHOW GLOBAL STATUS` command

```
SHOW GLOBAL STATUS LIKE "server_audit%";
+----------------------------+----------------------------------+
| Variable_name              | Value                            |
+----------------------------+----------------------------------+
| server_audit_active        | ON                               |
| server_audit_current_log   | /usr/local/mysql/data/audittest |
| server_audit_last_error    |                                  |
| server_audit_writes_failed | 0                                |
+----------------------------+----------------------------------+
```

Questions

Web, Doc & Knowledge Base:
www.mariadb.org
www.mariadb.com

Downloads:
www.skysql.com/downloads
https://mariadb.com/resources/
https://downloads.mariadb.org/

Ralf Gebhardt
ralf.gebhardt@skysql.com