Who did what, when, where and how

MySQL Audit Logging

Jeremy Glick & Andrew Moore

20/10/14

PERCONA LIVE

Intro

Hello

!

Intro

- Jeremy Glick
  - MySQL DBA
  - Head honcho of Chicago MySQL meetup
  - 13 years industry experience

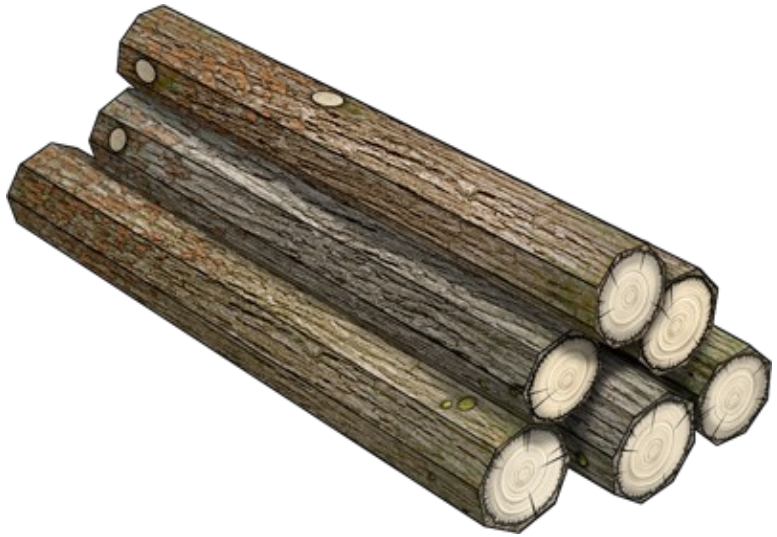
Intro

- Andrew Moore
  - Senior MySQL DBA
  - 5+ years in MySQL world
  - T-shirt and sticker collector
  - Organizer SW UK MySQL meetup

WTF?

- Why Log?
- What to Log?
- How [not] to Log

Logs



[timestamp]: [some useful data]

Why Log?

- Compliance and security
- Debug
- Insight

Compliance & Security

- Who is accessing sensitive data?
- What actions are they performing?

  - HIPAA
  - SOX
  - PCI DSS

Typically the main reason for audit logging

Compliance & Security

- No circumventing the audit logging solution
- Unable to disable logging
- Logging on by default
- Logging is not preventative

Regulatory Compliance

Database Auditing Requirements of Regulations

Audit Requirement	**SOX**	**PCI DSS**	**HIPAA**
Access to sensitive data **(SELECT)**		X	X
Modification of sensitive data **(INSERT,UPDATE,DELETE)**	X		
Schema Changes **(CREATE, ALTER, DROP)**	X	X	X
Security Auth **(GRANT, REVOKE)**	X	X	X
Security Exceptions **(Failed Logins)**	X	X	X

Source: Database Administration 2nd Edition, Craig Mullins

Debugging

- Development
- Production troubleshooting
- Retrospective investigation

Insight

- Aggregation
- Trending
- Capacity planning

What to Log

- Access (logins)
- Everything
- Targeted

How to Log

- Custom code
  - MySQL plugin
- Off the shelf plugins
  - MariaDB
  - Percona
  - McAfee
- Workarounds

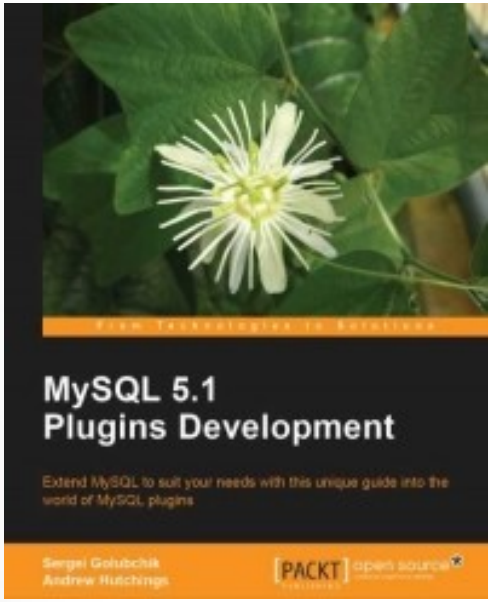
MySQL's Pluggable Audit Interface

- Available as of MySQL 5.5.3
- Audit interface notifies plugin of these operations:
  - Message written to general log
  - Message written to error log
  - Query results sent to client

* https://dev.mysql.com/doc/refman/5.6/en/audit-plugins.html

How to Log

- Custom code



Andrew Hutchings: http://linuxjedi.co.uk/

Other refs;

Oracle: http://goo.gl/9FCeGp

Openark: http://goo.gl/harxVU

How [not] to Log

- Parse logs
  - General
  - Slow
  - Binary
- Sniff the wire/proxy
- Half baked
  - init_connect
  - In schema
  - Triggers

Audit Solutions

- Open source solutions
  - MariaDB
  - Percona
  - McAfee
- Proprietary solutions
  - Oracle
  - Greensql
  - imperva

Installation

Plugin installation

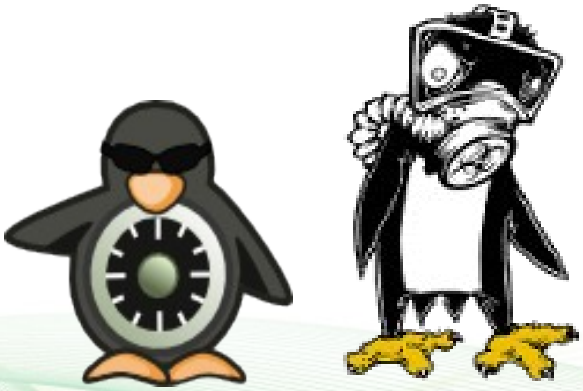
- INSTALL PLUGIN ***plugin_name*** SONAME= ***'shared_lib_name.so'***;
- plugin-load=***plugin_name=shared_lib_name.so***
- mysqld --plugin-load=***'plugin_name'='shared_lib_name.so'***
- **plugin_name**=FORCE

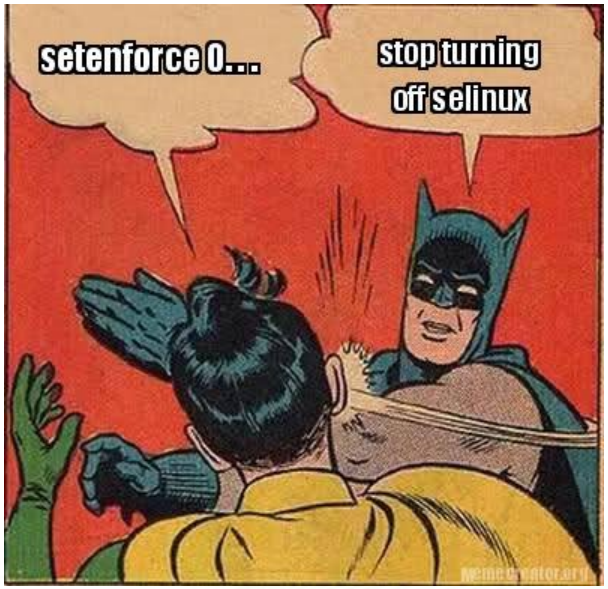
Installing An Audit Plugin

Troubleshooting installation

Check the **mysql error log** for evidence of issues starting the plugin. In some cases, you may have to make changes to SELinux or AppArmor so MySQL can write to the audit file.

- chcon
- Audit2allow
- Setsebool





MariaDB Audit Plugin

- Pros
  - Compatible with MariaDB, MySQL and Percona Server
  - Open Source & built on the audit api
  - Supported by MariaDB team
  - Status variables exposed
  - User filtering possible

- Cons
  - Logs passwords in plain text
  - No object filtering

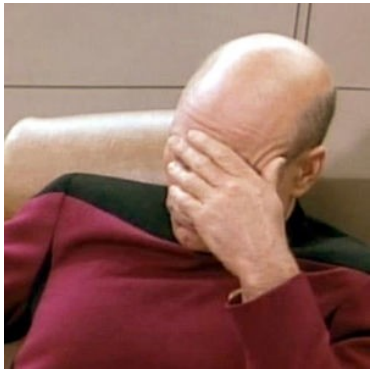
MariaDB Audit Plugin

- Events


```
20141101 13:33:26,5a11919fea9a,rdba,172.17.0.97,5,14,QUERY,,'show
databases',0
20141101 13:34:15,5a11919fea9a,rdba,172.17.0.97,5,15,QUERY,,'CREATE
DATABASE audit_test',0
20141101 13:34:36,5a11919fea9a,rdba,172.17.0.97,5,16,QUERY,,'create table
t1(id int, c1 varchar(10)) engine innodb',1046
20141101 13:34:44,5a11919fea9a,rdba,172.17.0.97,5,0,DISCONNECT,,,0
```

```
$ perror 1046
MySQL error code 1046 (ER_NO_DB_ERROR): No database selected
```

MariaDB Audit Plugin



```
mysql> GRANT ALL ON *.* TO 'mdb'@'172.%' IDENTIFIED BY
'facepalm';


20141031 23:32:24,5a11919fea9a,rdba, \
172.17.0.88,3,7,QUERY,mysql, \
'GRANT ALL ON *.* TO \'mdb\'@\'172.%\' IDENTIFIED BY \'facepalm\'',0
```

MariaDB Audit Plugin

- Status variables

```
mysql> show global status like '%audit%';
+--------------------------+---------------------------------+
| Variable_name            | Value                           |
+--------------------------+---------------------------------+
| Server_audit_active      | ON                              |
| Server_audit_current_log | /var/log/mysql/mariadb-audit.log |
| Server_audit_last_error  |                                 |
| Server_audit_writes_failed | 0                             |
+--------------------------+---------------------------------+
4 rows in set (0.00 sec)
```

Percona Audit Plugin

- Pros
  - Ships with Percona Server (no additional download)
  - Multiple output formats (XML,JSON,CSV,syslog)
  - Does not write passwords in plain text*!*
  - Open Source supported by Percona
  - Various performance modes

- Cons
  - XML only on early version
  - No object filtering
  - No user filtering
  - Only officially supported in PS

Percona Audit Plugin

- Events

```
mysql> select reverse(user) from mysql.user where user != '' order by rand();
```


```
{"audit_record":
        {"name":"Query",
        "record":"105834191_2014-10-29T12:06:50",
        "timestamp":"2014-10-31T23:43:42 UTC",
        "command_class":"select",
        "connection_id":"85",
        "status":0,
        "sqltext":"select reverse(user) from mysql.user where user != '' order by rand()",
        "user":"rdba[rdba] @  [172.17.0.91]",
        "host":"",
        "os_user":"",
        "ip":"172.17.0.91"}
}
```

Percona Audit Plugin

audit_log_strategy *(read only variable)*

- ASYNCHRONOUS = async logging, uses buffer
- PERFORMANCE = ascync, (drops requests if buffer is full)
- SEMISYNCHRONOUS = sync logging, uses OS caching
- SYNCHRONOUS = sync() each request

McAfee Audit Plugin

- Pros
  - Compatible with MySQL and Percona Server
  - Widest version support, 5.1+
  - Flexible filtering
  - Great community support
  - Compatible with `DAM`
- Cons
  - MariaDB 10 compatibility issues
  - Binary hooking access pattern
  - Installation hoops

McAfee Audit Plugin

- Events

```
mysql> select * from audit_test;

{"msg-type":"activity",
        "date":"1414851690462",
        "thread-id":"3",
        "query-id":"29",
        "user":"rdba",
        "priv_user":"rdba",
        "ip":"172.17.0.104",
        "cmd":"select",
        "objects":[{"db":"pluk","name":"audit_test","obj_type":"TABLE"}],"query":"select *
from audit_test"}
}
```

McAfee Audit Install

Demo

Replication

Mcafee

- Slaves log replicated transactions by default
- Whitelist blank user "{}" to prevent logging of replicated transactions

Percona

- Not logged

MariaDB

- Not logged

Log File Storage

- Secure storage (hardware encryption, FS encryption)
- Sign logs to ensure they have not been altered
- Set permissions correctly at OS level
- Store offsite (encrypted of course)
- Store on read only media

Summary

General best practices

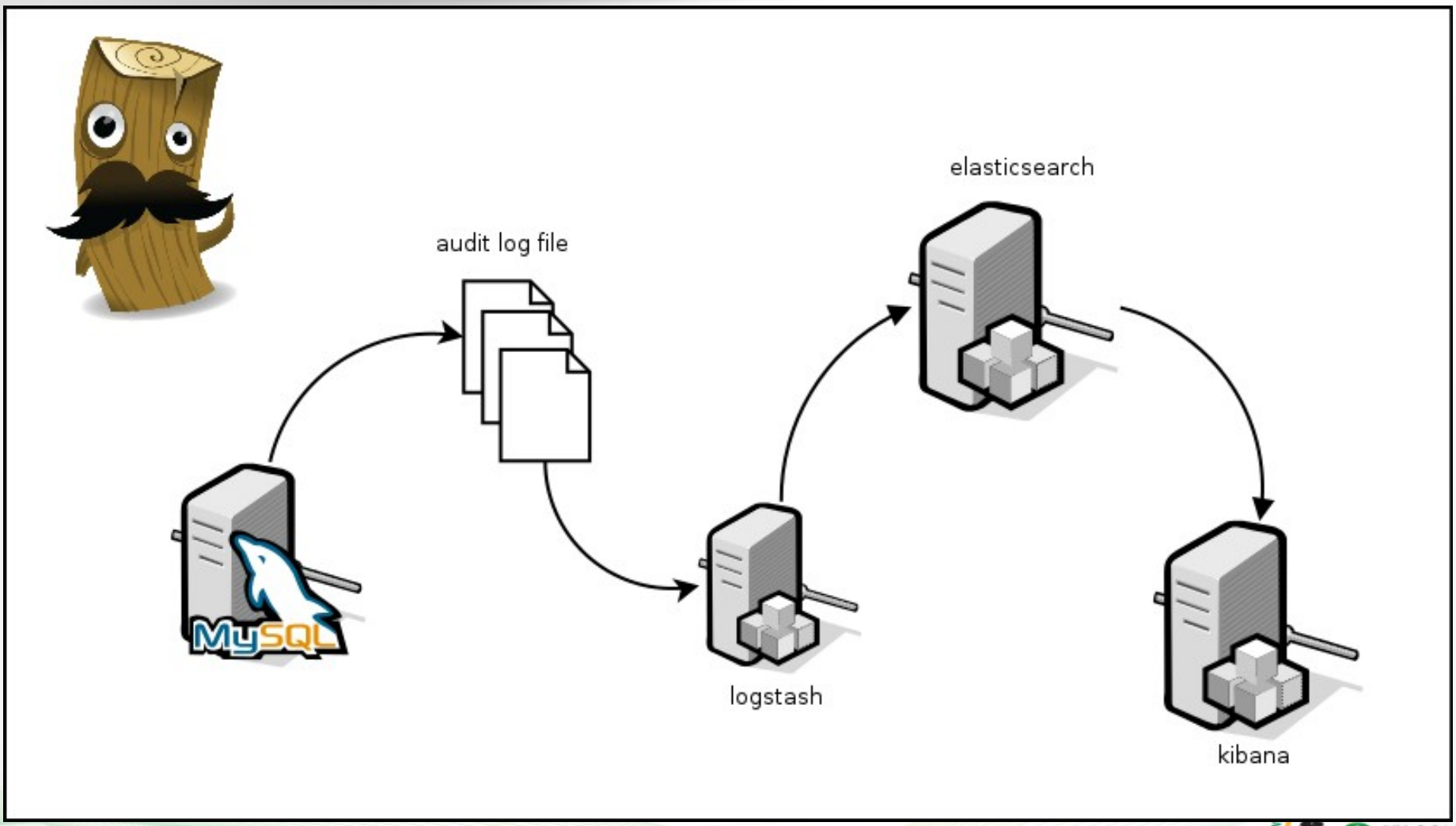
- Utilize the log rotation facilities/logrotate script
- Sequential logging lives away from random access.
- Use FS with journalling to be crash safe(r)
- Synchronizing writes to the disk hurts a lot.

Log Aggregation

ELK+ (Elasticsearch, Logstash, Kibana)

- Elasticsearch (search and analytics engine)
- Logstash (collect, parse and store log events)
- Kibana (easily visualize and search indexed data)
- + (Nagios,Ganglia,hipchat,irc,statsd...)

Standard ELK pipeline



ELK config

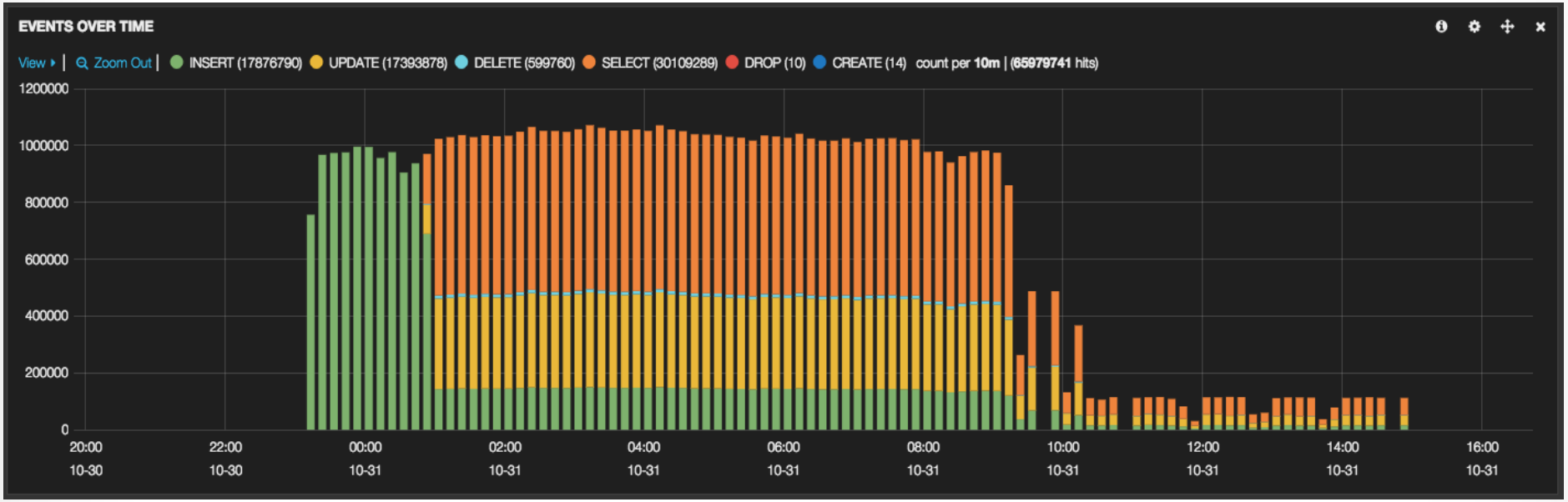
/etc/logstash/logstash.conf

```
input {
        file {
                path => "/var/log/mysql/audit.log"
                type => "mysql-audit"
  }

filter {
        do_something
}

output {
        elasticsearch {
                cluster => "logstash"
                host => elasticsearch1
        }
}
```

Kibana Visuals



Thank you

Q&A