Using Percona Audit plugin in daily operation

By Lenny Andersen, DBA
Disclaimer

Perhaps this session is a bit more detailed than planned at first.

But not rocket science.
What is it?

• The plugin is installed (but not enabled) with Percona servers.
• It will log all activity on the server.
• Can be configured to fit different use cases.
• Lightweight
• Not a log for performance tuning
Reasons to do audit logging

• The need for documentation on database usage.
• Having a documentation to do forencics in case of data theft.
• Getting a better understanding of data usage.
• Troubleshooting!
• I’m sure there’s a lot of other reasons.
Obstacles for making the logs useful.

- The raw output is bit verbose (xml, json, csv)
- Flat files are not very searchable
- Very storage consuming.
Solution

ClickHouse

• Data easily structured in a table
• Very very quick when searching
• Very good compression ratio
Demo

• Enable and configure Percona Audit Plugin
Considerations on the Plugin

- Output format (CSV, JSON, XML)
- Syslog or to local disk
- Do you want to log EVERYTHING?
  - Remember the consequences
- All settings for the plugin are described at
Topology and Workflow

1. Rotate log
2. Copy logs
3. Import logs
Demo

• Rotating and rsyncing the files
Importing the files into ClickHouse Database

- Format is JSON. Easy but ....
- Not one JSON object. Each line is a JSON object
- The origin of the file is not included in the audit log

Solution
- Fairly simple JSON parser (binary written in Go)
- Wrapped into a bash script
- Reading the ingress dir one file at a time.
- Available at Github (binary and sourcecode)
Demo

- Importing the files into ClickHouse
Using the data

• ClickHouse CLI gives easy access
• Investigate a timestamp query by query
• Follow a user
• Follow a host
• Follow a connection

• Obvious to implement into Grafana
Story time

Tellings from the trenches
What the heck is going on?
Security incidents

100! I meant 50-100 times!
There is something wrong with the database
There is something wrong with the database

<table>
<thead>
<tr>
<th>time</th>
<th>command_class</th>
<th>sqltext</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021-02-17 10:44:38</td>
<td>select</td>
<td>select blah blah from table blah blah</td>
</tr>
<tr>
<td>2021-02-17 09:43:27</td>
<td>set_option</td>
<td>SET NAMES utf8 COLLATE 'utf8_general_ci'</td>
</tr>
<tr>
<td>2021-02-17 09:43:27</td>
<td>set_option</td>
<td>SET sql_select_limit=1</td>
</tr>
<tr>
<td>2021-02-17 09:43:27</td>
<td>set_option</td>
<td>SET SESSION TRANSACTION ISOLATION LEVEL READ COMMITTED</td>
</tr>
<tr>
<td>2021-02-17 09:43:27</td>
<td>set_option</td>
<td>SET SESSION TRANSACTION READ WRITE</td>
</tr>
<tr>
<td>2021-02-17 09:43:27</td>
<td>set_option</td>
<td>SET character_set_results=NULL</td>
</tr>
<tr>
<td>2021-02-17 09:43:27</td>
<td>set_option</td>
<td>SET character_set_connection=utf8mb4</td>
</tr>
<tr>
<td>2021-02-17 09:43:27</td>
<td>set_option</td>
<td>SET character_set_client=utf8mb4</td>
</tr>
<tr>
<td>2021-02-17 09:43:27</td>
<td>set_option</td>
<td>SET collation_connection='utf8mb4_general_ci'</td>
</tr>
</tbody>
</table>
Useful links

• Percona Audit Plugin documentation

• Log importer
  • https://github.com/LennyAndersen/clickhouse-audit-import

• Grafana Clickhouse plugin
  • https://grafana.com/grafana/plugins/vertamedia-clickhouse-datasource/
Thanks!

Any questions?

You can find me at:

lenny@bdbafh.dk