Integrate MySQL Server

EventTracker Enterprise
Abstract

This guide provides instructions to configure MySQL to send the logs to EventTracker Enterprise. It supports the following MySQL flavors: MariaDB and Percona MySQL.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise, and MySQL Server 5.7, MariaDB 10.1 and Percona MySQL 5.6.31.

Target Audience

MySQL users, who wish to forward logs to EventTracker Manager.
# Table of Contents

Abstract .................................................................................................................................................. 1

Scope .................................................................................................................................................. 1

Target Audience .................................................................................................................................. 1

Overview ............................................................................................................................................. 3

Pre-requisite ....................................................................................................................................... 3

Configuration for sending logs to EventTracker .............................................................................. 3

1. MySQL Windows Configuration .................................................................................................. 4

   Configure log file monitor (LFM) for monitoring MySQL .......................................................... 6

2. MySQL Centos 7 Configuration .................................................................................................. 10

EventTracker Knowledge Pack (KP) ................................................................................................. 12

Category .......................................................................................................................................... 12

Reports ............................................................................................................................................. 13

Alerts .............................................................................................................................................. 19

Import MySQL Knowledge Pack into EventTracker .................................................................... 20

Category .......................................................................................................................................... 21

Alerts ............................................................................................................................................... 23

Templates ....................................................................................................................................... 24

Reports .......................................................................................................................................... 25

Verify Knowledge Pack in EventTracker ....................................................................................... 27

Categories ....................................................................................................................................... 27

Alerts ............................................................................................................................................... 27

Templates ....................................................................................................................................... 28

Reports .......................................................................................................................................... 29

Create Dashboards in EventTracker ............................................................................................... 30

Schedule Reports ............................................................................................................................ 30

Create Dashlets ............................................................................................................................... 33

Sample Dashboards ......................................................................................................................... 37
Overview

MySQL, the most popular Open Source SQL database management system, is developed, distributed, and supported by Oracle Corporation.

EventTracker collects and analyses the queries executed and enlightens an administrator about database management, user management and table management.

Pre-requisite

- EventTracker Enterprise v7.x for reports and alerts should be installed.
- EventTracker Enterprise v8.x for configuring reports, alerts and flex dashboards should be installed.
- MySQL database should be installed.
- EventTracker agent should be installed on Windows MySQL database system.
- Syslog should be enabled on Centos 7 MySQL machine.
- Firewall between EventTracker manager and MySQL system should be off or made exception for port 14505.

NOTE: For Percona MySQL integration guide, Please check the following link:


Below is the configuration for MySQL Server 5.7 and MariaDB 10.1.

Configuration for sending logs to EventTracker

NOTE: The below configuration applies to MySQL 5.7 and MariaDB 10.1 and is supported on Microsoft Windows and Centos 7.

1. On Windows: MySQL logs are consumed through Log File Monitoring (LFM).
2. On Centos 7: MySQL logs are forwarded using Syslog
1. MySQL Windows Configuration

a. To enable server auditing connect to MySQL database, login using administrative credentials.

```
C:\Program Files\MariaDB 10.1\bin> mysql -u root -p
Enter password: ********
```

Figure 1

b. **server_audit.dll** plugin is required to enable auditing, so check the plugins directory and run the query **SHOW VARIABLES LIKE 'plugin_dir';**

```
MariaDB [(none)]> SHOW VARIABLES LIKE 'plugin_dir';
+----------------------|---------------------------+
| Variable_name        | Value                     |
+----------------------|---------------------------+
| plugin_dir           | C:\Program Files\MariaDB 10.1\lib\plugin\ | 
+----------------------|---------------------------+
| rov in set (0.00 sec)
```

Figure 2

c. If you do not find the plugin file inside your plugins directory, download it and place it in the plugins directory manually.

d. Install the plugin using command **install plugin server_audit soname 'server_audit.dll';**

 e. To confirm the plugin is installed and enabled, run the query **show plugins;**

```
+--------+--------------------------+--------------------------+
| PLUGIN  | ACTIVE | AUDIT | server_audit.dll |
| GPL    |         |       |                  |
+--------+--------------------------+--------------------------+
```

Figure 3

f. Set the following on MySQL database

```
SET GLOBAL server_audit_events='CONNECT,QUERY,TABLE';
SET GLOBAL server_audit_logging=ON;
SET GLOBAL server_audit_output_type=FILE;
```

g. To see the currently set variables use the command **show global variables like "server_audit%";**
h. To verify auditing enabled, run query: Show global status like ‘serverAudit%’;

i. Now, click my.ini configuration setting file of MySQL.

j. In my.ini configuration setting file of MySQL, set the following:

```
server_audit_logging=ON
server_audit_output_type=file
server_audit_events=CONNECT,QUERY,TABLE
```

k. In Run, type ‘services.msc’ and then click OK. Restart the MySQL service.

l. Now connect to MySQL database and execute the queries by performing activities, logs are written into server_audit.log file in the installation path of the MySQL.
Configure log file monitor (LFM) for monitoring MySQL

To perform LFM configuration, deploy the EventTracker agent on MySQL machine. For this, please refer EventTracker Agent installation guide. After installation of the ET agent, check the steps to configure LFM.

1. Select the **Start** button, select **Prism Microsystems**, and then select **EventTracker Control Panel**.
2. Click the icon **EventTracker Agent Configuration**.

![EventTracker Agent Configuration](image)

Figure 6
3. Click the button **Add File Name** and select the **server_audit.log file** which has been generated and then click **OK**.
4. Select **Get All Existing Log Files** option.
5. In **Select Log File Type** drop down, select the **Multiline** option.
6. Enter the path of the MySQL logs.

![Figure 7](image)

7. Click the **OK** button.
8. Now, click the **Search String** button.
9. Select **Add String**.
10. Select the string to configure, that needs to be searched in the selected logs. If any of the string matches, then a log is generated.

```
EventTracker Agent Configuration

Select Systems
PC-1

Apply the following settings to specified Agents

Manager destinations:
PC-1

Log Backup  |  Performance  |  Network Connections
Managers   |  Event Filters |  System Monitor |  Monitor Processes |  Services
Logfile Monitor  |  File Transfer  |  Config Assessment  |  syslog FTP server

✓ Logfile Monitor

Search log files (various formats supported) for matching patterns specified here. Both individual files as well as folders can be monitored for matching entries. Matches cause an event to be generated.

<table>
<thead>
<tr>
<th>Logfile Name</th>
<th>File Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Program Files\MySQL\data\server_audit.log</td>
<td>MULTILI...</td>
</tr>
</tbody>
</table>
```

Figure 10

11. Click **Save**

Logs will be sent to the EventTracker Enterprise.
2. MySQL Centos 7 Configuration

a. Log into Centos machine with administrative privileges.
b. Connect to MySQL database and verify for the audit plugin.

```
[root@centos7-vm05 ~]# mysql -u root -p
Enter password:
```

Figure 11

c. `server_audit.so` plugin is required to enable auditing. So check the plugins directory and run the query `show variables like 'plugin_dir';`

```
MariaDB [(none)]> show variables like 'plugin_dir';
+----------------+-----------+
| Variable_name  | Value     |
|----------------+-----------+
| plugin_dir     | /usr/lib64/mysql/plugin/ |
+----------------+-----------+
1 row in set (0.28 sec)
```

Figure 12

d. If you do not find the plugin file inside your plugins directory, download it and place it in the plugins directory manually.

e. Install the plugin using command `install plugin server_audit soname 'server_audit.so';`

f. To confirm the plugin is installed and enabled, run the query `show plugins;`

```
<table>
<thead>
<tr>
<th>SERVER_AUDIT</th>
<th>ACTIVE</th>
<th>AUDIT</th>
<th>server_audit.s</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPL</td>
<td></td>
<td></td>
<td>server_audit.so</td>
</tr>
</tbody>
</table>
```

Figure 13

g. Access `my.cnf` configuration file, available at `/etc` folder.

h. Edit using text editor `# vi my.cnf` file and enable the following:

```
server_audit_events='CONNECT, QUERY, TABLE'
server_audit_file_path=server_audit.log
server_audit_logging = ON
server_audit_output_type = SYSLOG
server_audit_syslog_facility=LOG_LOCAL6
```
i. To see the currently set variables with the command **show global variables like "server_audit%;"**

![Image](image1.png)

Figure 14

j. To verify auditing is enabled, run the query: **Show global status like 'server_audit%;';**

![Image](image2.png)

Figure 15

k. Access `rsyslog.conf` on folder `/etc`. Enable syslog using text editor `#vi rsyslog.conf` file.

**NOTE:** Syslog can be enabled using TCP or UDP protocol.

Syslog enabled with TCP

![Image](image3.png)

Figure 16
Syslog enabled with UDP

![Figure 17](image)

**NOTE:** The IP address should be that of EventTracker Manager Machine and the port ‘514’.

1. Restart MySQL service `# /etc/init.d/mysqld restart` and connect to MySQL database. Run the queries and the logs generated will be forwarded to EventTracker Manager Machine through Syslog.

**EventTracker Knowledge Pack (KP)**

Once logs are received in to EventTracker; Reports and Alerts can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support MySQL.

**Category**

- **MySQL: Authentication failure**
  This category provides information related to user authentication failure.

- **MySQL: Authentication success**
  This category provides information related to user authentication success.

- **MySQL: User logoff**
  This category provides information related to user logoff from the database.

- **MySQL: User password changed**
  This category provides information related to password reset to an existing user account.

- **MySQL: Root logins**
  This category provides information related to root logins.

- **MySQL: Root logon failure**
  This category provides information related to root logon failure.

- **MySQL: Create database**
  This category provides information related to creation of database by the user.
- **MySQL: Delete database**
  This category provides information related to database dropped by the user.

- **MySQL: Create user**
  This category provides information related to create and configure a database user.

- **MySQL: Delete user**
  This category provides information related to remove a database user and optionally remove the user’s objects.

- **MySQL: Rename user**
  This category provides information related to rename existing MySQL user accounts.

- **MySQL: Create table**
  This category provides information related to create a table in a database.

- **MySQL: Delete table**
  This category provides information related to delete a table and all rows in the table.

- **MySQL: Rename Table**
  This category provides information related to when the tables are renamed by the user.

- **MySQL: Insert into Table**
  This category provides information related to insert new records in a table.

- **MySQL: Update Table**
  This category provides information related to update existing records in the table.

- **MySQL: Alter Table**
  This category provides information related to add, delete or modify columns in an existing table.

- **MySQL: Privileges change**
  This category provides information related to providing access or privileges and the removing access on the database objects to the users.

### Reports

- **MySQL- User authentication failed**
  This report provides the information related to the authentication failure, when user enters the wrong credentials and fails to connect the database.
Logs Considered:

- **MySQL-User authentication success**
  This report provides the information related to authentication success, when user connects the database with valid credentials.

Logs Considered:

- **MySQL-User logoff**
  This report provides the information related to user logged off from the database.
Logs Considered:

- **MySQL-User password changed**
  This report provides the information related to user password changed by the administrator.

Logs considered:
• **MySQL-Database management**  
This report provides information related to database management when user creates and drops the database.

Logs Considered:

![Figure 26](image)

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>User Name</th>
<th>Client Host</th>
<th>Action</th>
<th>Database Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/21/2016 05:44:30 PM</td>
<td>ESXWIN2K12R2VM3</td>
<td>tommy</td>
<td>PC1.Contoso.com</td>
<td>CREATE</td>
<td>sbh</td>
</tr>
<tr>
<td>09/21/2016 06:58:09 PM</td>
<td>ESXWIN2K12R2VM3</td>
<td>hillary</td>
<td>PC5.Contoso.com</td>
<td>CREATE</td>
<td>rbi</td>
</tr>
</tbody>
</table>

![Figure 27](image)

• **MySQL-User management**  
This report provides the information related to user management when administrator creates, drops and renames the user details.
Logs Considered:

- **MySQL-Table management**
  This report provides information related to table management when user creates, drops, renames, updates, inserts and alters the table.
Logs considered:

Figure 30

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>User Name</th>
<th>Client Host</th>
<th>Action</th>
<th>Database</th>
<th>TableName</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/21/2016 12:33:36 PM</td>
<td>ESXWIN2K12R2VM3</td>
<td>root</td>
<td>localhost</td>
<td>rename</td>
<td>mysql</td>
<td>students to student</td>
</tr>
<tr>
<td>09/21/2016 05:41:41 PM</td>
<td>ESXWIN2K12R2VM3</td>
<td>bob</td>
<td>PC4.Contoso.com</td>
<td>DROP</td>
<td>kotak</td>
<td>pet</td>
</tr>
<tr>
<td>09/21/2016 05:10:17 PM</td>
<td>ESXWIN2K12R2VM3</td>
<td>bob</td>
<td>PC4.Contoso.com</td>
<td>INSERT</td>
<td>kotak</td>
<td>pet</td>
</tr>
<tr>
<td>09/21/2016 05:33:47 PM</td>
<td>ESXWIN2K12R2VM3</td>
<td>bob</td>
<td>PC4.Contoso.com</td>
<td>UPDATE</td>
<td>kotak</td>
<td>hr</td>
</tr>
<tr>
<td>09/21/2016 05:35:17 PM</td>
<td>ESXWIN2K12R2VM3</td>
<td>bob</td>
<td>PC4.Contoso.com</td>
<td>ALTER</td>
<td>kotak</td>
<td>hr ADD EID INT</td>
</tr>
</tbody>
</table>

Figure 31
- **MySQL: Privilege management**
  This report provides information related to privilege management when administrator has granted or revoked the privileges from the particular user.

Logs Considered:

![Figure 32](image)

![Figure 33](image)

**Alerts**

- **MySQL: Service down** - This alert is generated when MySQL service is shutdown by the administrator.
- **MySQL: User authentication failed** – This alert is generated when user enters wrong credentials to connect MySQL database.
- **MySQL: Privilege change** – This alert is generated when administrator grants or revokes the privileges to the user.
- **MySQL: User created** – This alert is generated when administrator creates the user.
• MySQL: Delete database – This alert is generated when administrator deletes the database.
• MySQL: Delete table – This alert is generated when administrator deletes the table.
• MySQL: User password reset – This alert is generated when administrator resets the user password.

Import MySQL Knowledge Pack into EventTracker

1. Launch EventTracker Control Panel.
2. Double click Export Import Utility icon, and then click the Import tab.

NOTE: Import the following KP items in the specified sequence.

• Category
• Alerts
• Templates
• Reports
Category

1. Click **Category** option, and then click the browse button.
2. Locate the All MySQL group of categories.iscat file, and then click the **Open** button.
3. Click the **Import** button to import the categories. EventTracker displays success message.

4. Click the **OK** button and then click the **Close** button.
Alerts

1. Click the **Alert** option, and then click the browse button.
2. Locate the **All MySQL group of alerts.isalt** file, and then click the **Open** button.

![Figure 37](image)

3. Click the **Import** button to import the alerts.
   
   EventTracker displays success message.

![Figure 38](image)
4. Click the OK button and then click the Close button.

Templates

1. Click the Admin menu, and then click Parsing rule.

2. Select Template tab, and then click on Import option.

3. Click on Browse button.

4. Locate All MySQL group of templates.ettd file, and then click the Open button.
5. Now select the check box and then click on ‘Import’ option. EventTracker displays success message.

![Template(s) imported successfully](image)

6. Click on OK button.

### Reports

1. Click Report option, and then click the browse button.

2. Locate All MySQL group of reports.issch file, and then click the Open button.
3. Click the **Import** button to import the reports.

   EventTracker displays success message.

4. Click the **OK** button, and then click the **Close** button.
Verify Knowledge Pack in EventTracker Categories

1. Logon to EventTracker Enterprise.
2. Click the Admin dropdown, and select Category.
3. In the Category Tree, expand MySQL group folder to see the imported categories.

Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin dropdown, and then click Alerts.
3. In the Search field, enter 'MySQL', and then click the Go button.
   Alert Management page will display all the imported MySQL alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

5. Click the **OK** button, and then click the **Activate now** button.

**NOTE:** You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

**Templates**

1. Click the **Admin** menu, and then click **Parsing rule**.

2. Select **Template** tab, and then click on **Import** option.
Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then Configuration.
4. In Report Groups Tree to view imported Scheduled Reports, scroll down and click MySQL group folder.

Reports are displayed in the Reports configuration pane.
Create Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.

2. Navigate to Reports>Configuration.
3. Select **MySQL** in report groups. Check ‘**Defined**’ option.

4. Click on ‘**schedule**’ to plan a report for later execution.
5. Choose appropriate time for report execution and in Step 8 check ‘Persist data in Eventvault explorer’ box.
6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

7. Proceed to next step and click **Schedule** button.

8. Wait for scheduled time or generate report manually.

Create Dashlets

1. **EventTracker 8** is required to configure flex dashboard.

2. Open **EventTracker** in browser and logon.

3. Navigate to **Dashboard>Flex**. Flex Dashboard pane is shown.

4. Click ☰ to add a new dashboard. Flex Dashboard configuration pane is shown.
5. Fill fitting title and description and click **Save** button.
6. Click 🛠 to configure a new flex dashlet. Widget configuration pane is shown.
7. Locate earlier scheduled report in **Data Source** dropdown.
8. Select **Chart Type** from dropdown.
9. Select extent of data to be displayed in **Duration** dropdown.
10. Select computation type in **Value Field Setting** dropdown.
11. Select evaluation duration in **As Of** dropdown.
12. Select comparable values in **X Axis** with suitable label.
13. Select numeric values in **Y Axis** with suitable label.
14. Select comparable sequence in **Legend**.
15. Click **Test** button to evaluate. Evaluated chart is shown.
16. If satisfied, click **Configure** button.

17. Click ‘customize’ ✖️ to locate and choose created dashlet.

18. Click ✪ to add dashlet to earlier created dashboard.
Sample Dashboards

For below dashboard **DATA SOURCE: MySQL: Database management**

1. **MySQL: Database management**

   - **WIDGET TITLE:** MySQL Database management
   - **CHART TYPE:** Donut
   - **AXIS LABELS [X-AXIS]:** Database Name
   - **Label Text:** Database Name
   - **LEGEND [Series]:** Action
   - **SELECT:** All

   ![MySQL Database Management Dashboard](image)

   **Figure 60**
For below dashboard **DATA SOURCE: MySQL: User management**

2. **MySQL: User management**

- **WIDGET TITLE:** MySQL User management
- **CHART TYPE:** Donut
- **AXIS LABELS [X-AXIS]:** MySQL User Name
- **Label Text:** MySQL User Name
- **LEGEND [Series]:** Action
- **SELECT:** All

![MySQL User Management Chart](image)

*Figure 61*