EventTracker
Secure. Comply. Succeed.

Integrate Percona MySQL

EventTracker Enterprise

Publication Date: Oct. 5, 2016

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

About this Guide

This guide will facilitate a **Percona MySQL** user to send SYSLOG logs to **EventTracker Enterprise**.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise 7.x or later, Percona MySQL 5.6.31.**

Audience

Administrators who want to monitor **Percona MySQL** using EventTracker Enterprise.

Table of Contents

Introduction

Percona MySQL is an open source software company specializing in MySQL support, consulting, managed services, and training. It aims to retain close compatibility to the official MySQL releases, while focusing on performance and increased visibility into server operations. Percona MySQL freely includes a number of scalability, availability, security and backup features only available in MySQL's commercial Enterprise edition.

Pre-requisites

- **EventTracker 7.x or later** should be installed.
- **Percona MySQL software** should be installed in the Centos machine**.**
- **Port 514** should be allowed on firewall**.**

Configuration

AUDIT CONFIGURATION

1. Install Percona MySQL 5.6.31 into your system.

2. Open Linux terminal.

3. Connect to MySQL.

   - **Run the following command:**

     #MySQL -u root –p XXXXXXXX

     You are prompted for your password which was given by you.

4. Audit Log plugin is shipped with Percona MySQL Server, but it is not installed by default.

   - **To enable the plugin, you must run the following command:**

     MySQL>INSTALL PLUGIN audit_log SONAME 'audit_log.so';

5. You can check if the plugin is loaded correctly by running:

   MySQL>SHOW PLUGINS;

   - **Audit log should be listed in the output as shown below:**

```
+-------------------------------+---------+-------------------+------------
-+---------+
| Name                          | Status  | Type              | Library
| License |
+-------------------------------+---------+-------------------+------------
-+---------+
...
| audit_log                     | ACTIVE  | AUDIT             | audit_log.so
| GPL     |
+-------------------------------+-----------------------------------------
```

6. In order to check the audit log format and audit log handler, use the below command.

   MySQL> show global variables like 'audit%;

   - **You get the below output: (BEFORE audit settings)**

```
Variable_name           Value
audit_log_buffer_size   1048576
audit_log_file          /var/log/mysql/audit.l
og
audit_log_flush         OFF
audit_log_format        OLD
audit_log_handler       FILE
audit_log_policy        ALL
audit_log_rotate_on_size  1073741824

audit_log_rotations       10
audit_log_strategy        ASYNCHRONOUS

audit_log_syslog_facility LOG_USER
audit_log_syslog_ident    percona-
audit
audit_log_syslog_priority LOG_INFO
```

7. To exit from MySQL terminal-

   MySQL>exit

8. Open Linux terminal.
9. Edit the my.cnf.

NOTE: Percona MySQL stores the data files in **/var/lib/MySQL/** by default. You can find the configuration file that is used to manage Percona MySQL in **/etc/my.cnf**.

- **Hence use the following command to edit my.cnf.**

  #Vi my.cnf

- **Add the settings which is marked inside the red box.**

```
# join_buffer_size = 128M
# sort_buffer_size = 2M
# read_rnd_buffer_size = 2M
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock

# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0

# Recommended in standard MySQL setup
#sql_mode=NO_ENGINE_SUBSTITUTION,STRICT_TRANS_TABLES

[mysqld_safe]
log-error=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid
## Audit Logging ##
[mysqld]
audit_log_policy=ALL
audit_log_format=OLD
audit_log_handler=SYSLOG
#audit_log_file=/var/log/mysql/audit.log
#audit_log_rotate_on_size=1024M
#audit_log_rotations=10
-- INSERT --
```

Figure 1

10. To save:

    :wq

11. Start the service.

    - **You should start it by running:**

      #service MySQL start

12. Confirm that the service is running-

    - **You can check the service status by running:**

      #service MySQL status

13. Again login to MySQL to verify the audit settings.

#MySQL -u root –p XXXXXXXX

You are prompted for your password which was given by you.

14. In order to check the audit log format and audit log handler, use the below command:

    MySQL> show global variables like 'audit%';

- **You get the below output: (AFTER audit settings).**

```
Variable_name            Value
audit_log_buffer_size    1048576
audit_log_file           /var/log/mysql/audit.log
audit_log_flush          OFF
audit_log_format         OLD
audit_log_handler        SYSLOG
audit_log_policy         ALL
audit_log_rotate_on_size 1073741824
audit_log_rotations      10
audit_log_strategy       ASYNCHRONOUS
audit_log_syslog_facility LOG_USER
audit_log_syslog_ident   percona-audit
audit_log_syslog_priority LOG_INFO
```

MySQL>exit

SYSLOG CONFIGURATION

15. In Linux terminal of Percona MySQL.

- Use the commands as shown below:

  #Cd /etc
  # ls

- Check for rsyslog.conf

16. Edit the rsyslog.conf using the command as shown below:

    #vi rsyslog.conf

- Once the rsyslog.conf opens-

17. Scroll down and add the IP address and the port you want the logs to be forwarded, as shown below in red box.

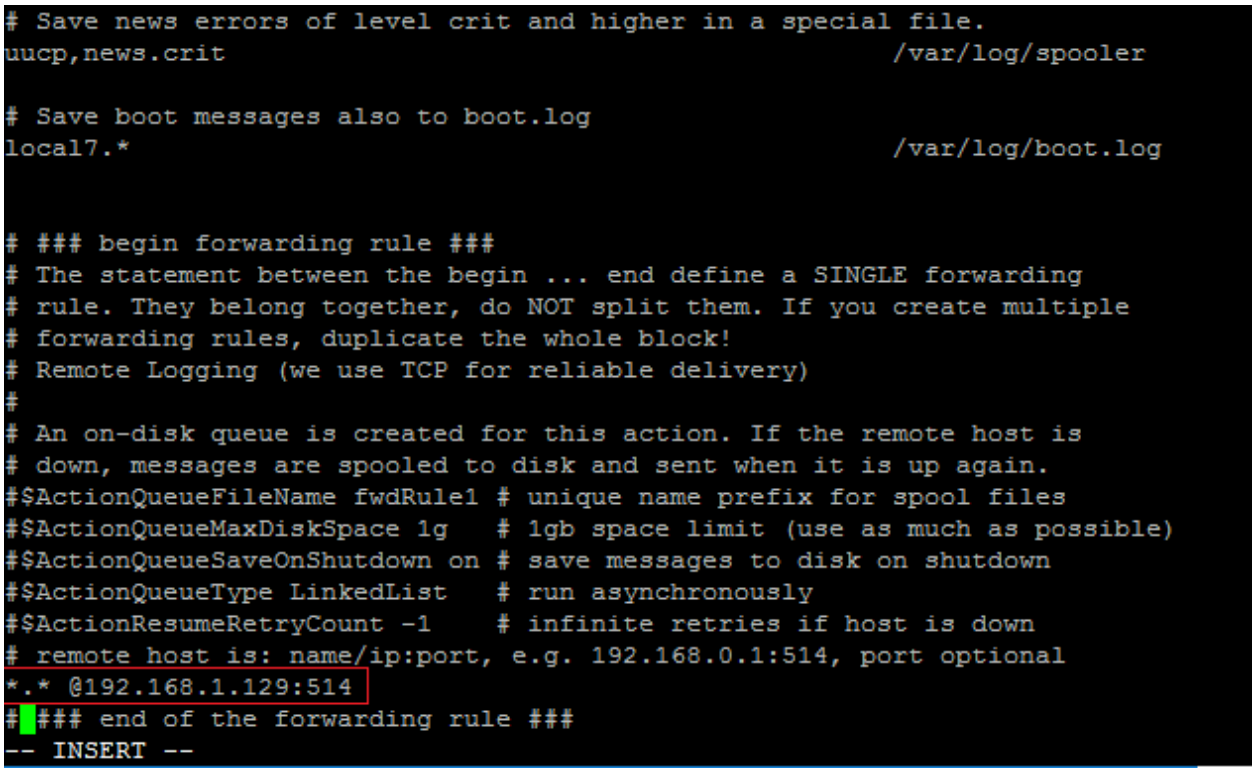


Figure 2

18. To save-

:wq

- **Once audit and syslogs are enabled, Percona MySQL logs are forwarded to EventTracker machine.**

EventTracker Knowledge Pack

Once Percona MySQL events are enabled and Percona MySQL events are received in EventTracker, Alerts and Reports can be configured in EventTracker.

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

Categories

- **Percona MySQL: Database management**
  This category gives information related to database management that is whether the database has been created or dropped by the user.

- **Percona MySQL: User authentication failed**
  This category gives information related to failed authentication that is whenever the user tries to login to MySQL with wrong credentials.

- **Percona MySQL: User authentication successful**
  This category gives information related to successful authentication where the user provides the right credentials to login to the MySQL.

- **Percona MySQL: Table management**
  This category gives information related to table management where the table has been updated, dropped, created and values are inserted.

- **Percona MySQL: User management**
  This category gives information related to user management that is when the user is created given permissions like grant or revoke or even delete the user.

- **Percona MySQL: Variable change**
  This category gives information related to variable changes that is whenever the user tries any change in variable of MySQL.

Alerts

- **Percona MySQL: User management**
  This alert is generated whenever the user has been created, dropped given permissions to the users like grant and revoke.

Reports

- **Percona MySQL-Database management**
  This report provides information related to database management that is whether the database has been created or dropped by the user.

  SAMPLE REPORT

LogTime	Host Name	User Name	Computer	Command Class	SQL Text	IP Address	Database
09/07/2016 04:28:22 PM	localhost	root[root] @ localhost []	192.168.1.119-SYSLOG	create_db	create database ..		test
09/07/2016 05:20:15 PM	localhost	root[root] @ localhost []	192.168.1.119-SYSLOG	drop_db	drop database iisc		
09/16/2016 03:03:25 PM	CONTOSO WKSTN-01	root[root] @ CONTOSO WKSTN-01	192.168.1.119-SYSLOG	create_db	CREATE SCHEMA `IISC`	192.168.1.129	TEST

Figure 3

SAMPLE LOG

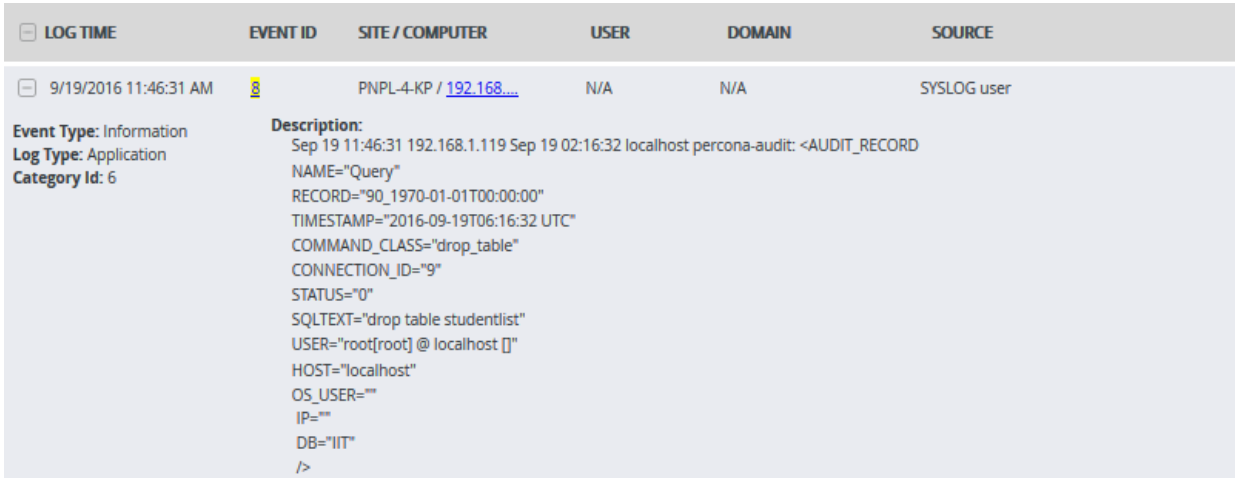


Figure 4

- **Percona MySQL-User authentication failed**
  This report provides information related to failed authentication that is whenever the user tries to login to MySQL by providing wrong credentials.

SAMPLE REPORT

LogTime	Host Name	User Name	Computer	IP Address	Database	Privileged User
09/07/2016 04:25:56 PM	localhost	michel	192.168.1.119-SYSLOG			root
09/16/2016 03:11:02 PM	CONTOSO WKSTN-01	ronaldino	192.168.1.119-SYSLOG	192.168.1.129	TEST	root

Figure 5

SAMPLE LOG

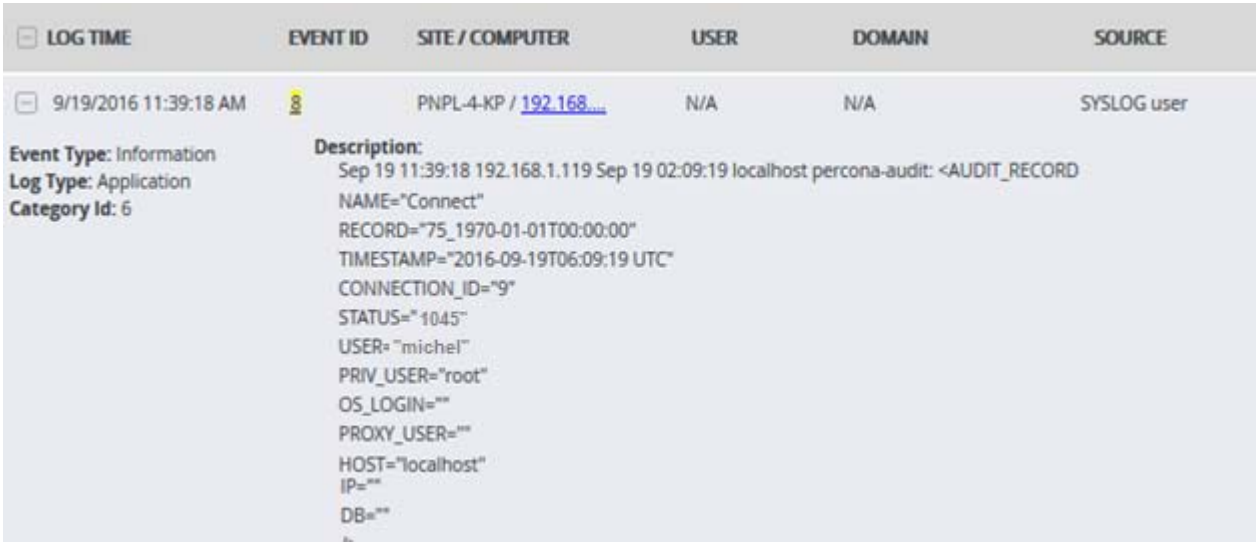


Figure 6

- **Percona MySQL-User authentication successful**
  This report provides information related to authentication success that is whenever the user login to MySQL by providing right credentials.

SAMPLE REPORT

LogTime	Host Name	User Name	Computer	Privileged User	IP Address	Database
09/07/2016 04:24:31 PM	localhost	johny	192.168.1.119-SYSLOG	root		
09/07/2016 04:25:42 PM	CONTOSO-WKSTN-01	christy	192.168.1.119-SYSLOG	root	192.168.1.129	TEST

Figure 7

SAMPLE LOG

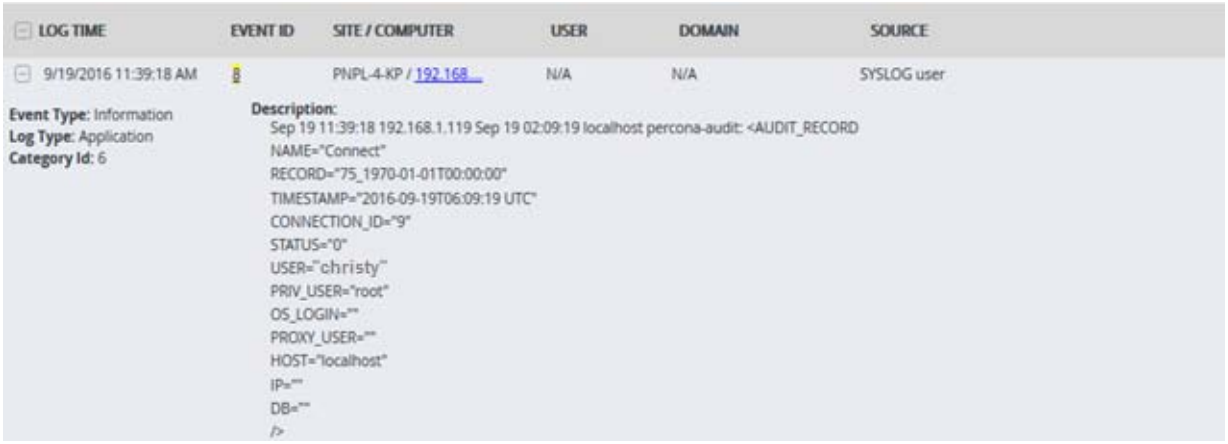


Figure 8

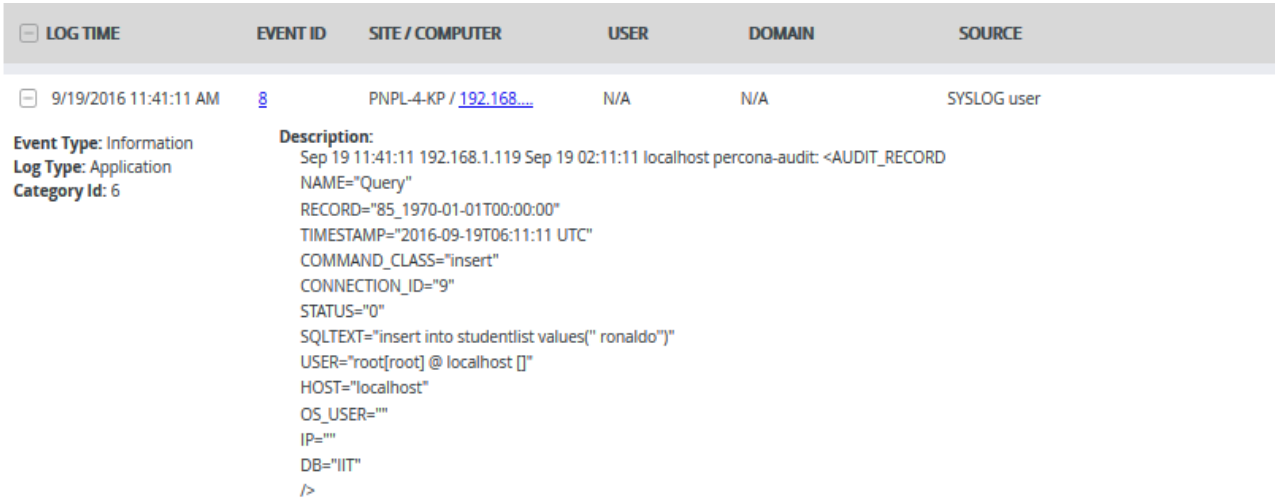
- **Percona MySQL-Table management**
  This report provides information related to table management where the table has been updated, dropped, created and values are inserted.

SAMPLE REPORT

LogTime	Host Name	User Name	Computer	Command Class	SQL Text	IP Address	Database
09/07/2016 04:33:48 PM	localhost	root[root] @ localhost []	192.168.1.119-SYSLOG	create_table	create table iisc
(
StudentName		test
09/07/2016 04:36:31 PM	localhost	root[root] @ localhost []	192.168.1.119-SYSLOG	drop_table	drop table iisc		test
09/07/2016 05:24:16 PM	CONTOSO WKSTN-01	root[root] @ CONTOSO WKSTN-01 [192.168.1.129]	192.168.1.119-SYSLOG	create_table	create table IISC
(&#10 ;name varchar(300),&	192.168.1.129	AQUIRED
09/07/2016 05:30:55 PM	localhost	root[root] @ localhost []	192.168.1.119-SYSLOG	insert	INSERT INTO IISC		AQUIRED
09/07/2016 05:32:17 PM	CONTOSO WKSTN-01	root[root] @ CONTOSO WKSTN-01 [192.168.1.129]	192.168.1.119-SYSLOG	insert	INSERT INTO IISC	192.168.1.129	AQUIRED
09/07/2016 05:39:01 PM	localhost	root[root] @ localhost []	192.168.1.119-SYSLOG	update	update IISC set name='john'		AQUIRED
09/08/2016 05:02:21 PM	CONTOSO WKSTN-01	root[root] @ CONTOSO WKSTN-01 [192.168.1.129]	192.168.1.119-SYSLOG	drop_table	drop table IISC	192.168.1.129	TEST

Figure 9

SAMPLE LOG



LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
9/19/2016 11:41:11 AM	8	PNPL-4-KP / 192.168....	N/A	N/A	SYSLOG user

Event Type: Information
Log Type: Application
Category Id: 6

Description:
Sep 19 11:41:11 192.168.1.119 Sep 19 02:11:11 localhost percona-audit: <AUDIT_RECORD
NAME="Query"
RECORD="85_1970-01-01T00:00:00"
TIMESTAMP="2016-09-19T06:11:11 UTC"
COMMAND_CLASS="insert"
CONNECTION_ID="9"
STATUS="0"
SQLTEXT="insert into studentlist values('' ronaldo'')"
USER="root[root] @ localhost []"
HOST="localhost"
OS_USER=""
IP=""
DB="IIT"
/>

Figure 10

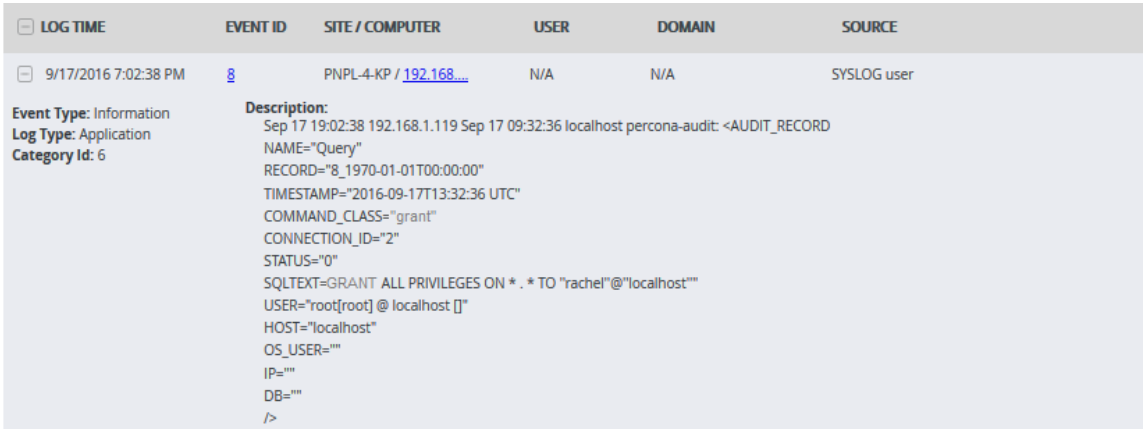
- **Percona MySQL-User management**
  This report provides information related to user management that is when the user is created given permissions like grant or revoke or even delete the user.

SAMPLE LOG

LogTime	Host Name	User Name	Computer	Command Class	SQL Text	IP Address	Database
09/08/2016 05:24:43 PM	CONTOSO WKSTN-01	root[root] @ CONTOSO WKSTN-01[192.168.1.129]	192.168.1.119-SYSLOG	create_user	CREATE USER 'Ronald'@'localhost' IDENTIFIED BY PASSWORD '*2D0B2321B6B0B78	192.168.1.129	TEST
09/08/2016 05:25:46 PM	CONTOSO WKSTN-01	root[root] @ CONTOSO WKSTN-01	192.168.1.119-SYSLOG	grant	grant create on TEST.IISC to	192.168.1.129	TEST
09/08/2016 05:26:53 PM	localhost	root[root] @ localhost []	192.168.1.119-SYSLOG	revoke	revoke create on TEST.IISC from		TEST
09/08/2016 05:27:13 PM	localhost	root[root] @ localhost []	192.168.1.119-SYSLOG	drop_user	drop user 'Ronald'@'localhost'		TEST

Figure 11

SAMPLE REPORT



LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
9/17/2016 7:02:38 PM	8	PNPL-4-KP / 192.168....	N/A	N/A	SYSLOG user

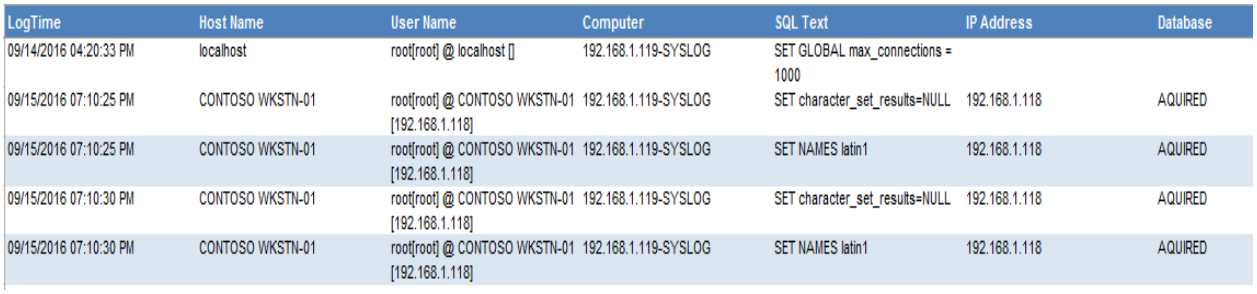
Event Type: Information
Log Type: Application
Category Id: 6

Description:
Sep 17 19:02:38 192.168.1.119 Sep 17 09:32:36 localhost percona-audit: <AUDIT_RECORD
NAME="Query"
RECORD="8_1970-01-01T00:00:00"
TIMESTAMP="2016-09-17T13:32:36 UTC"
COMMAND_CLASS="grant"
CONNECTION_ID="2"
STATUS="0"
SQLTEXT=GRANT ALL PRIVILEGES ON * . * TO "rachel"@"localhost""
USER="root[root] @ localhost []"
HOST="localhost"
OS_USER=""
IP=""
DB=""
/>

Figure 12

- **Percona MySQL-Variable change**
  This report provides information related to variable changes that is whenever the user tries any change in variable of MySQL.

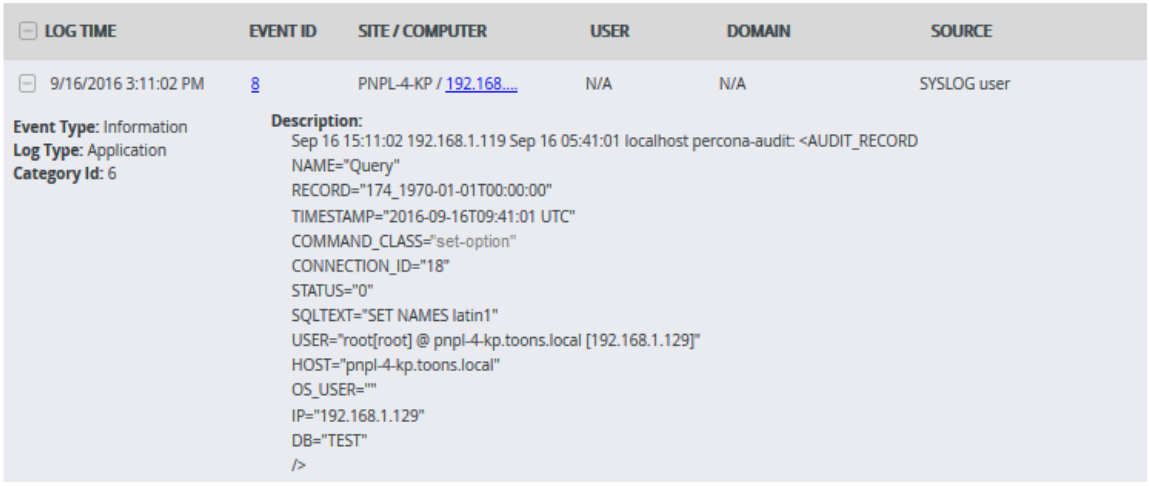
SAMPLE REPORT



LogTime	Host Name	User Name	Computer	SQL Text	IP Address	Database
09/14/2016 04:20:33 PM	localhost	root[root] @ localhost []	192.168.1.119-SYSLOG	SET GLOBAL max_connections = 1000		
09/15/2016 07:10:25 PM	CONTOSO WKSTN-01	root[root] @ CONTOSO WKSTN-01 [192.168.1.118]	192.168.1.119-SYSLOG	SET character_set_results=NULL	192.168.1.118	AQUIRED
09/15/2016 07:10:25 PM	CONTOSO WKSTN-01	root[root] @ CONTOSO WKSTN-01 [192.168.1.118]	192.168.1.119-SYSLOG	SET NAMES latin1	192.168.1.118	AQUIRED
09/15/2016 07:10:30 PM	CONTOSO WKSTN-01	root[root] @ CONTOSO WKSTN-01 [192.168.1.118]	192.168.1.119-SYSLOG	SET character_set_results=NULL	192.168.1.118	AQUIRED
09/15/2016 07:10:30 PM	CONTOSO WKSTN-01	root[root] @ CONTOSO WKSTN-01 [192.168.1.118]	192.168.1.119-SYSLOG	SET NAMES latin1	192.168.1.118	AQUIRED

Figure 13

SAMPLE LOG



LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
9/16/2016 3:11:02 PM	8	PNPL-4-KP / 192.168....	N/A	N/A	SYSLOG user

Event Type: Information
Log Type: Application
Category Id: 6

Description:
Sep 16 15:11:02 192.168.1.119 Sep 16 05:41:01 localhost percona-audit: <AUDIT_RECORD
NAME="Query"
RECORD="174_1970-01-01T00:00:00"
TIMESTAMP="2016-09-16T09:41:01 UTC"
COMMAND_CLASS="set-option"
CONNECTION_ID="18"
STATUS="0"
SQLTEXT="SET NAMES latin1"
USER="root[root] @ pnpl-4-kp.toons.local [192.168.1.129]"
HOST="pnpl-4-kp.toons.local"
OS_USER=""
IP="192.168.1.129"
DB="TEST"
/>

Figure 14

- **Percona MySQL-Failed events**
  This report provides information related to failed event that is anything other than zero in status is considered as failed events.

SAMPLE REPORT

LogTime	Host Name	User Name	Computer	Database	Command Class	IP Address	SQL Text	Privileged User
09/15/2016 06:52:32 PM	localhost	root[root] @ localhost []	192.168.1.119-SYSLOG		set_option		Set Host_Name = 192.168.1.119	
09/16/2016 02:49:21 PM	CONTOSO WKSTN-01	root	192.168.1.119-SYSLOG	TEST		192.168.1.129		root
09/16/2016 02:49:38 PM	CONTOSO WKSTN-01	root	192.168.1.119-SYSLOG			192.168.1.129		root
09/16/2016 02:49:53 PM	CONTOSO WKSTN-01	root	192.168.1.119-SYSLOG			192.168.1.129		root
09/16/2016 02:49:58 PM	CONTOSO WKSTN-01	root	192.168.1.119-SYSLOG	AQUIRED		192.168.1.129		root

Figure 15

SAMPLE REPORT

Figure 16

Importing Percona MySQL knowledge pack into EventTracker

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

   Import

   I. **Category**
   II. **Alerts**
   III. **Parsing Rules**
   IV. **Flex Reports**

NOTE: Importing should be in the same order as mentioned above.

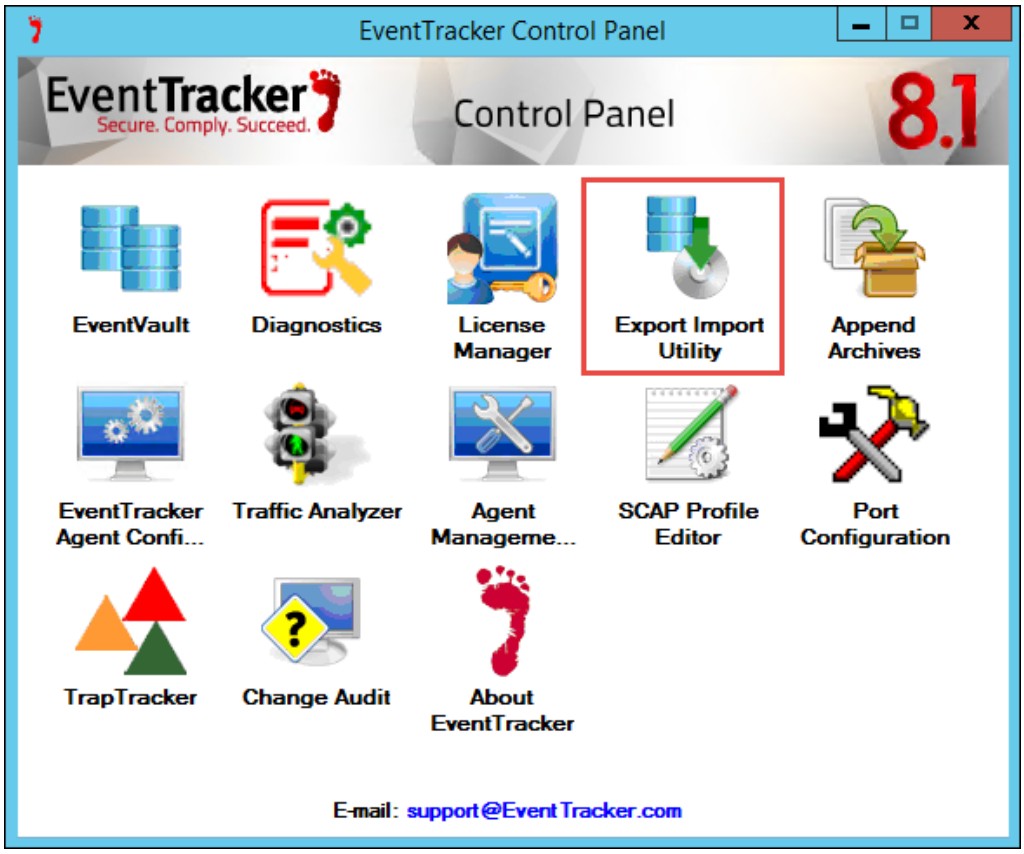


Figure 17

Category

1. Click **Category** option, and then click the browse  button.

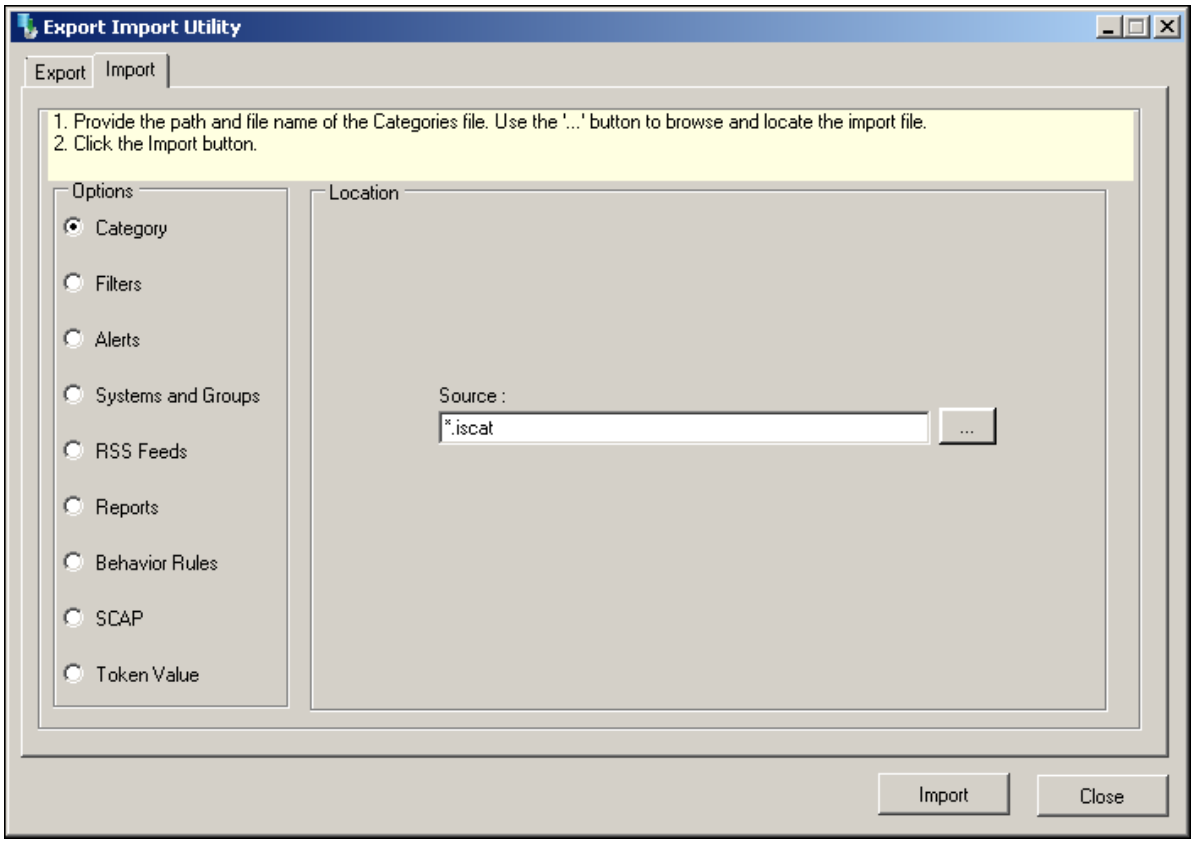


Figure 18

2. Locate **All Percona MySQL category.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

   EventTracker displays success message.

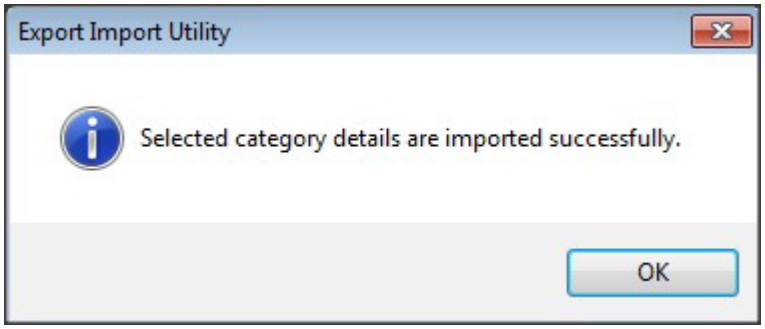


Figure 19

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

Alerts

1. Click **Alerts** option, and then click the **browse** button.

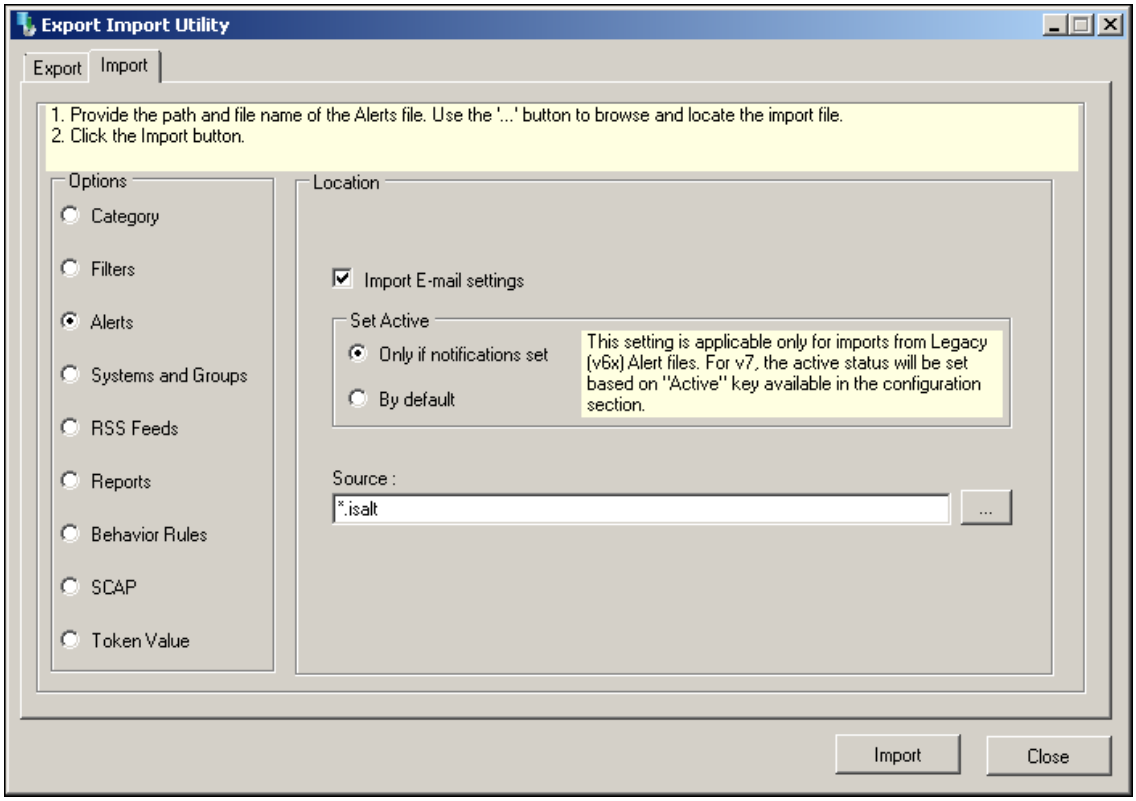


Figure 20

2. Locate **All Percona MySQL alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

   EventTracker displays success message.

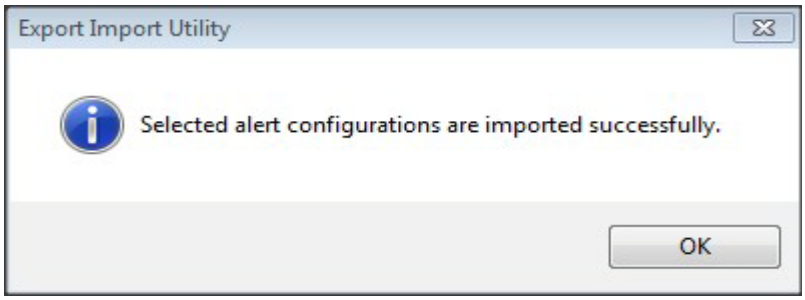


Figure 21

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

Parsing Rules

1. Click **Token value** option, and then click the **browse** button.

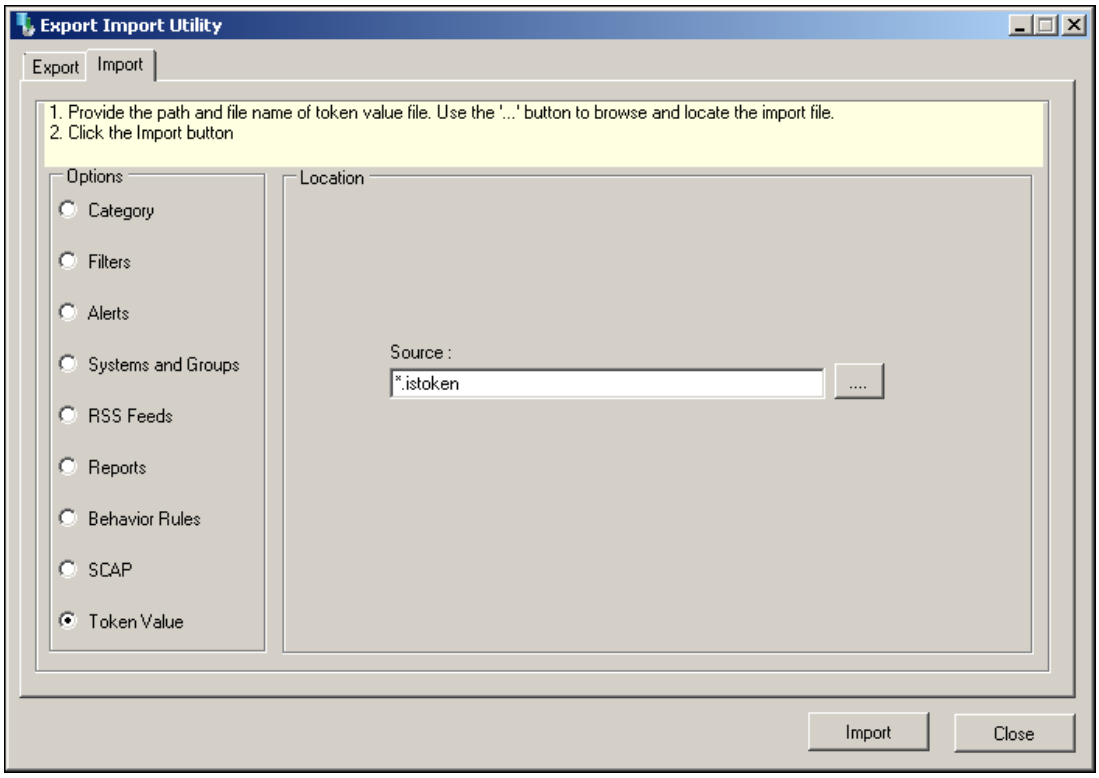


Figure 22

2. Locate **All Percona MySQL parsing rule.istoken** file, and then click the **Open** button.
3. To import tokens, click the **Import** button.

   EventTracker displays success message.

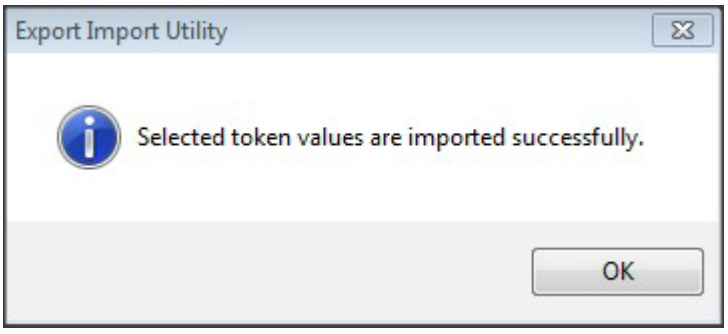


Figure 23

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

Flex Reports

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

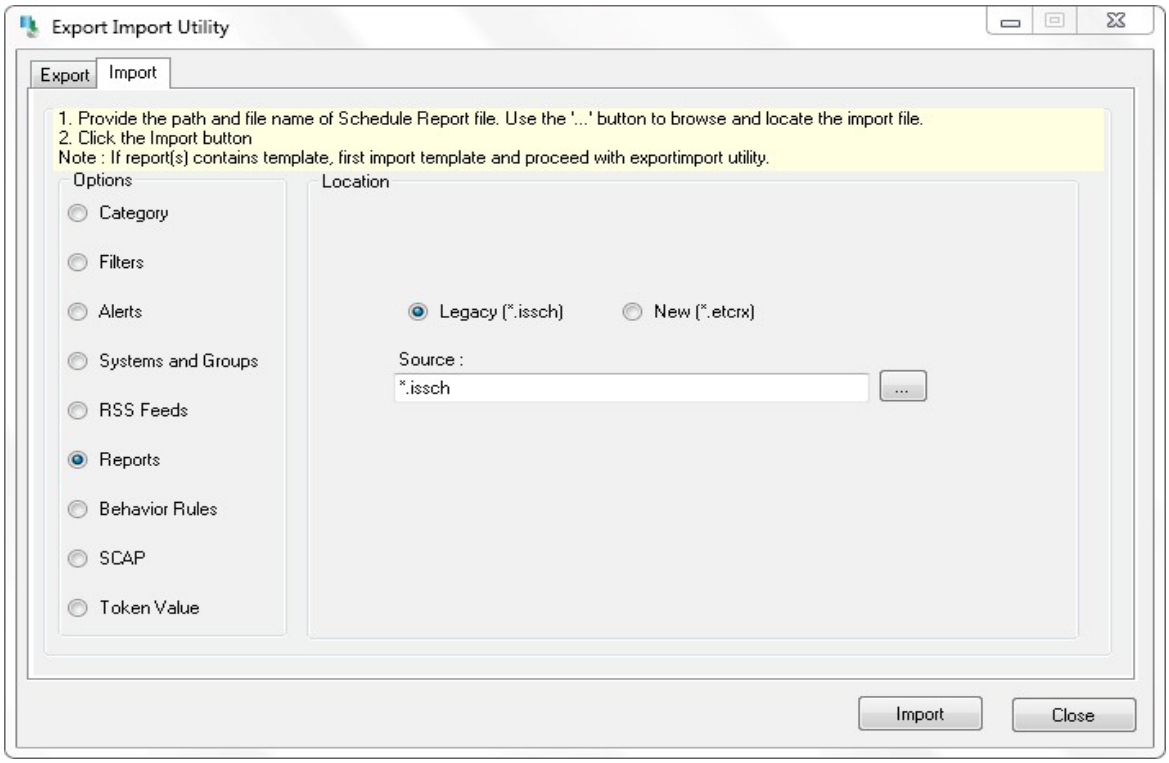


Figure 24

2. Locate **All Percona MySQL report.issch** file, and then click the **Open** button.
3. To import reports, click the **Import** button.

   EventTracker displays success message.

Figure 25

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

Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on '**Import**' option.

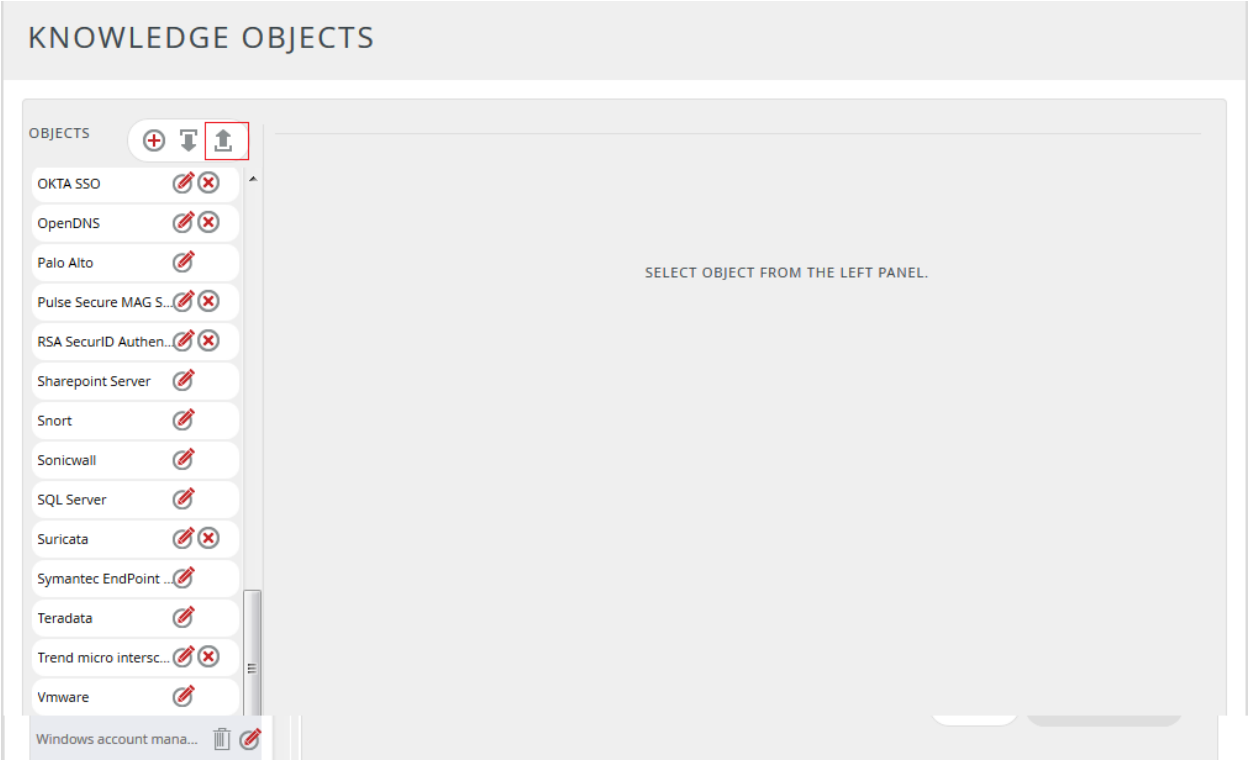


Figure 26

3. In **IMPORT** pane click on **Browse** button.

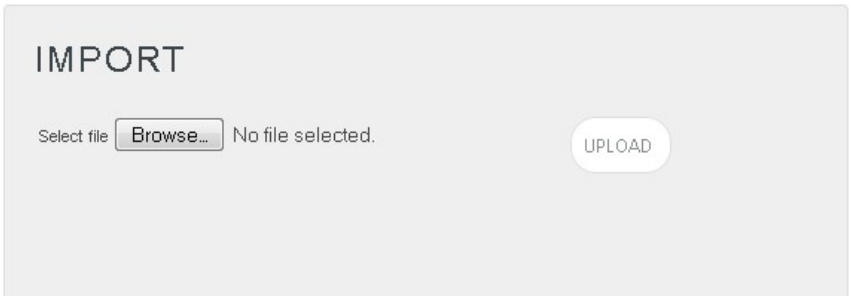


Figure 27

4. Locate **All Percona MySQL KO.etko** file, and then click the **UPLOAD** button.

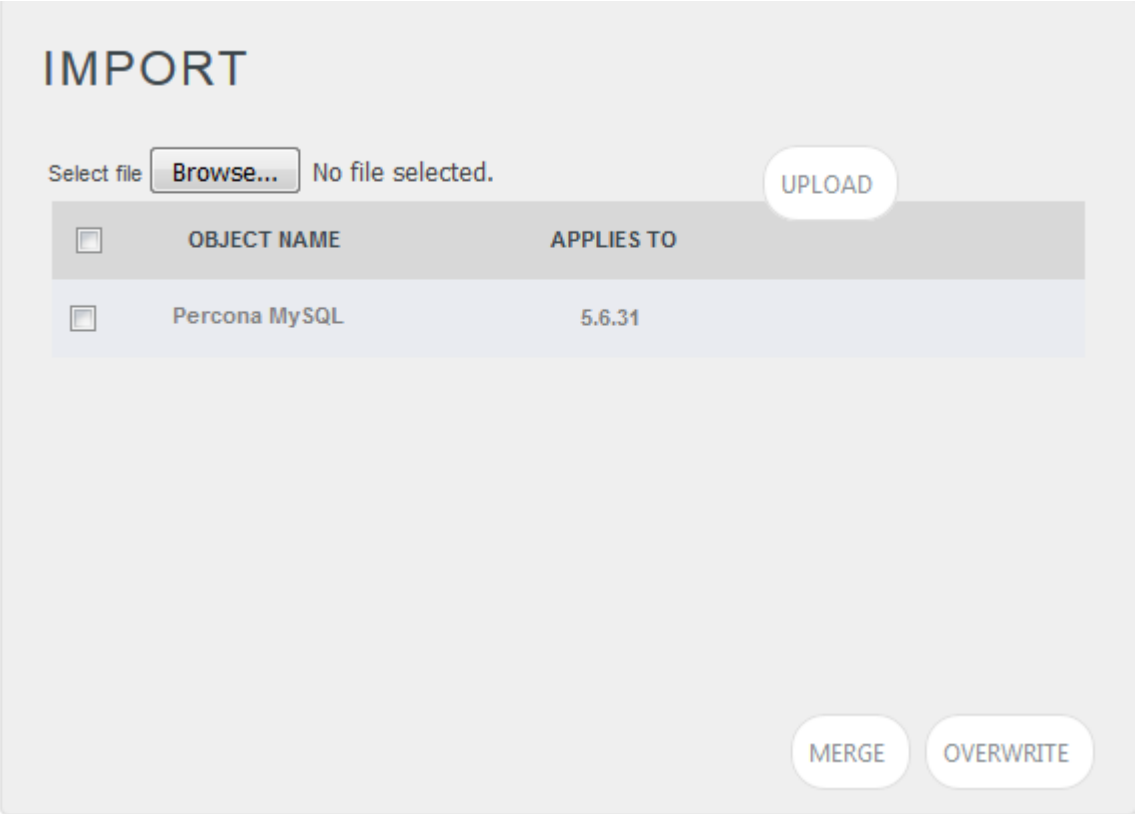


Figure 28

5. Now select the check box and then click on '**OVERWRITE**' option. EventTracker displays success message.

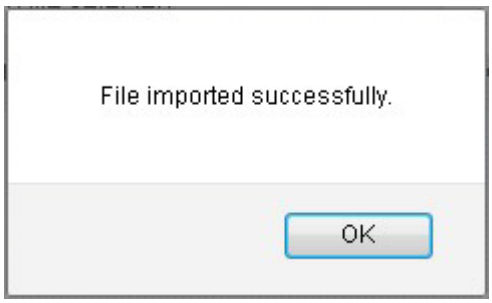


Figure 29

6. Click on **OK** button.

Verifying Percona MySQL knowledge pack in EventTracker

Categories

1. Logon to **EventTracker Enterprise Web Interface**.
2. Click the **Admin** menu, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand **Percona MySQL** group folder to view the imported categories.

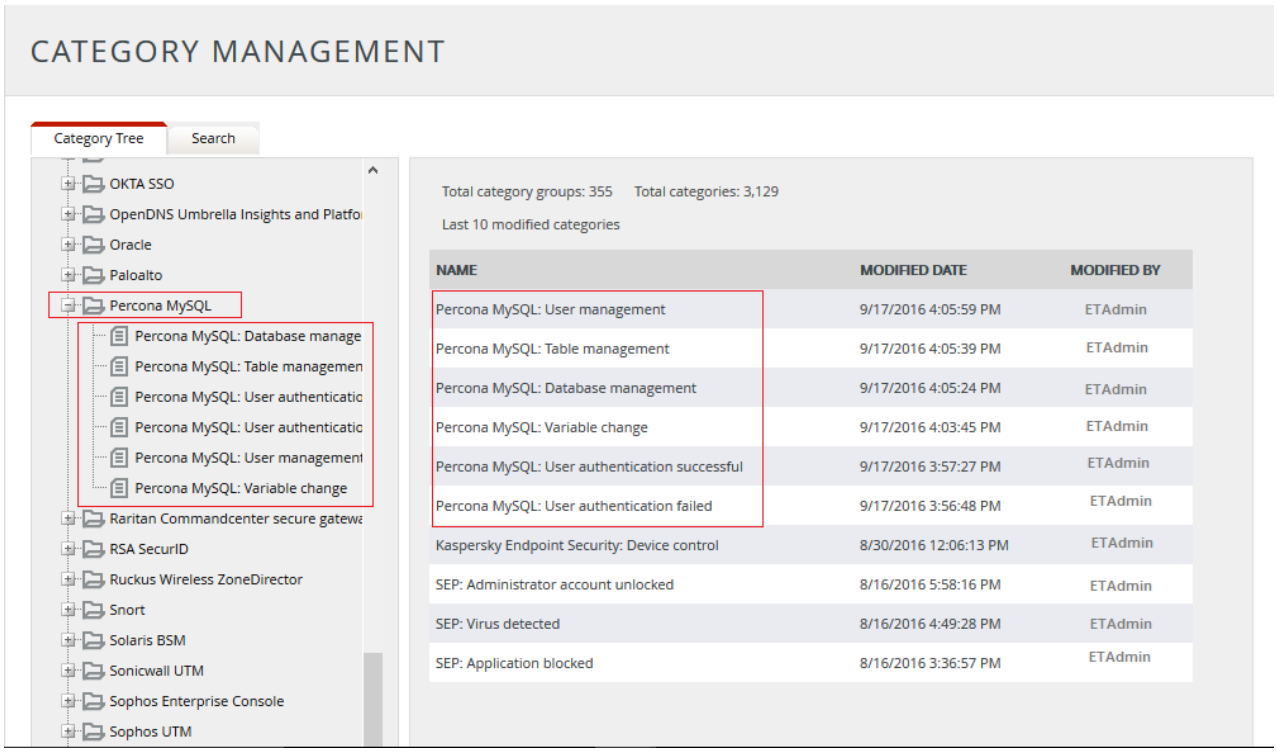


Figure 30

Alerts

1. Logon to **EventTracker Enterprise Web Interface**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In **Search** field, type '**Percona**", and then click the **Go** button.

Alert Management page will display all the imported **Percona MySQL** alerts.

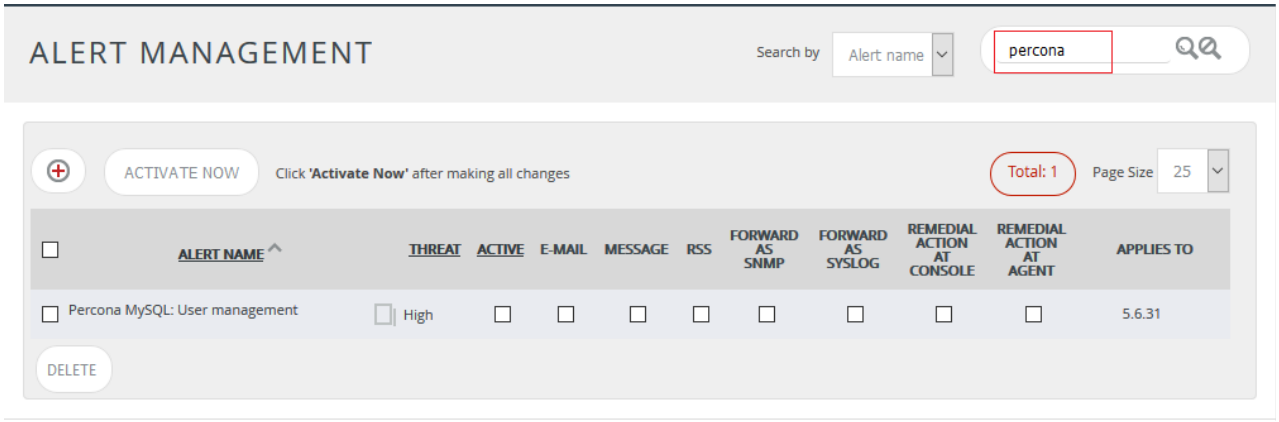


Figure 31

4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

Figure 32

5. Click **OK**, 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.

Tokens

1. Logon to **EventTracker Enterprise Web Interface**.
2. Click the **Admin** menu, and then click **Parsing Rules**.

The imported **Percona MySQL** tokens are added in Token-Value Groups list.

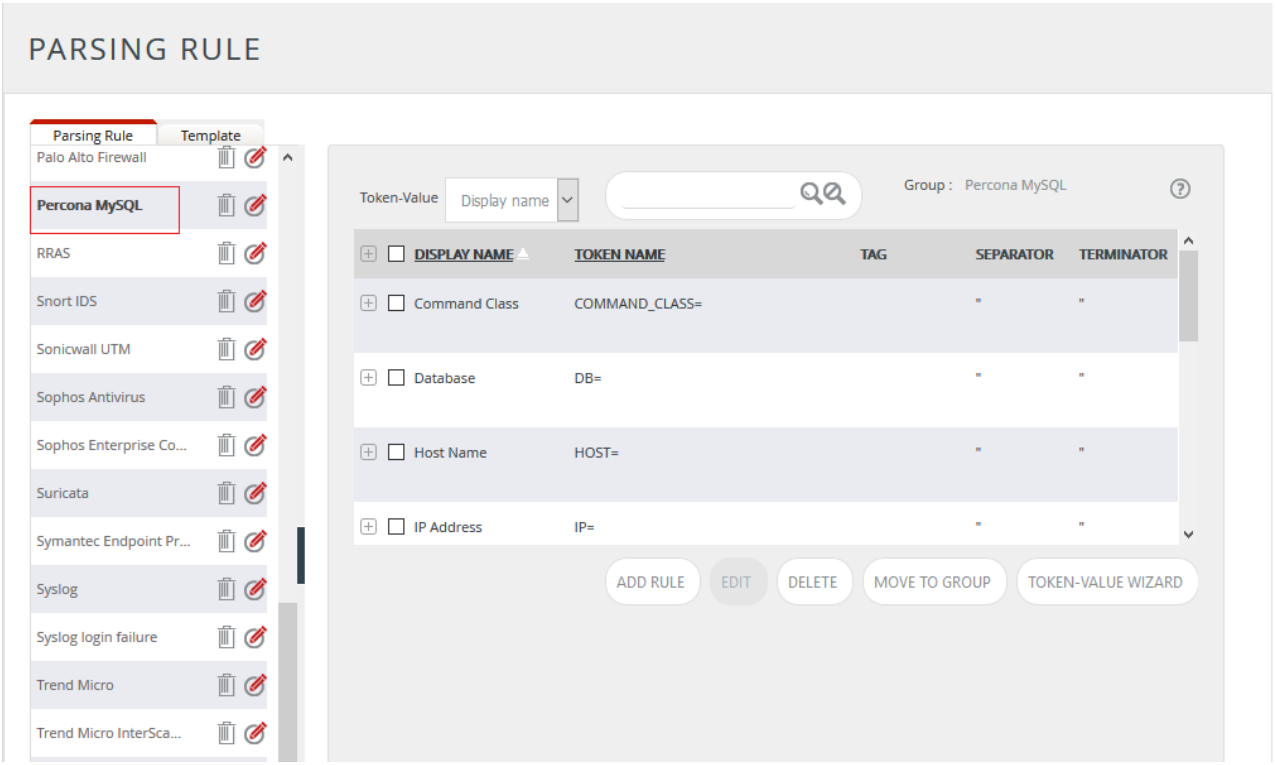


Figure 33

Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu, and then select **Configuration**.
3. In **Reports Configuration** pane, select **Defined** option.

   EventTracker displays **Defined** page.

4. In search box enter **Percona MySQL**, and then click the **Search** button.

   EventTracker displays Flex reports of **Percona MySQL.**

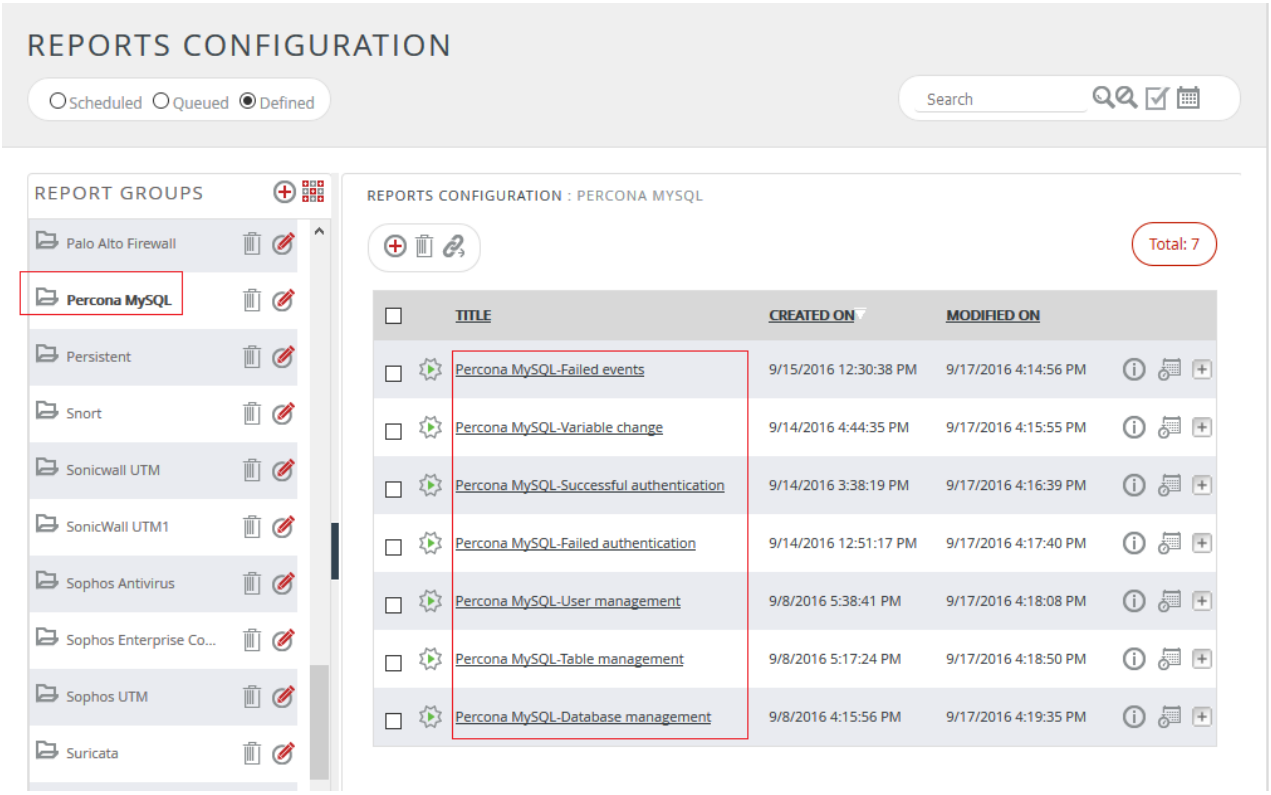


Figure 34

Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Scroll down and select **Percona MySQL** in **Objects** pane. Imported **Percona MySQL** object details are shown.

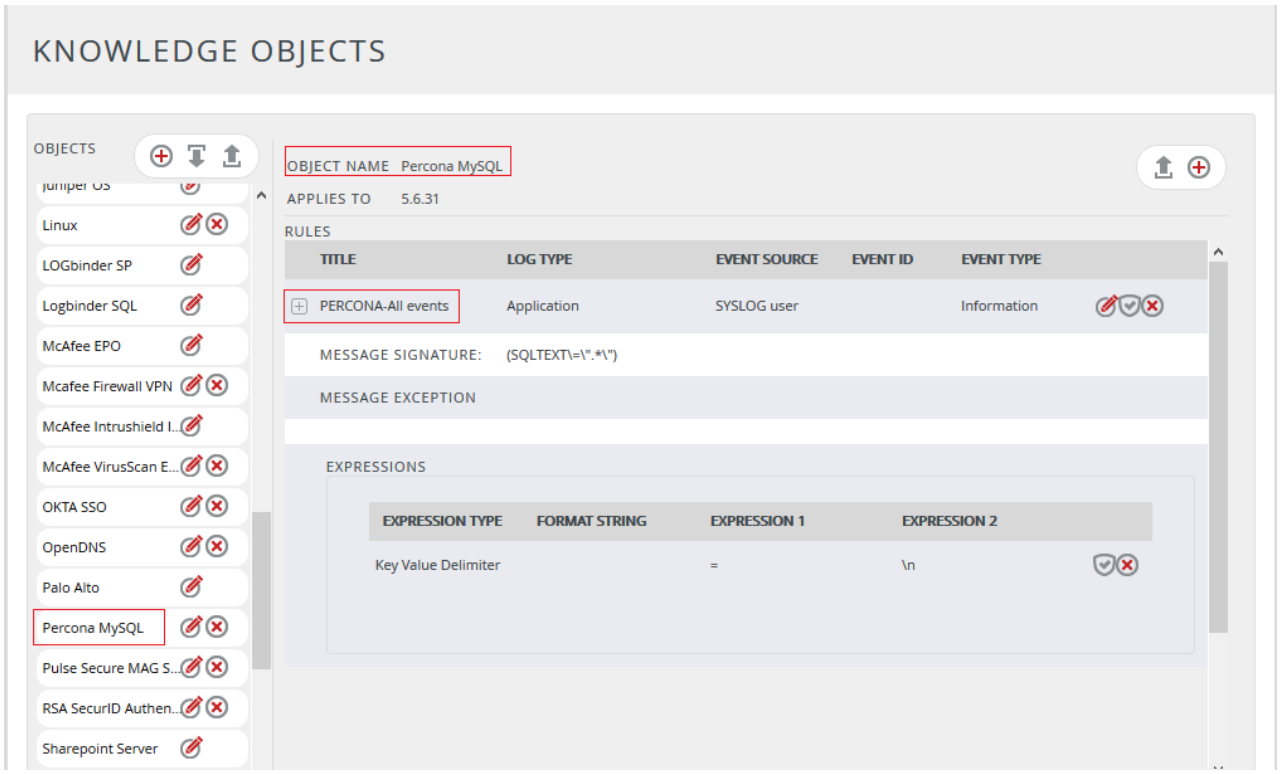


Figure 35

Create Flex Dashboards in EventTracker

NOTE: To configure the flex dashboards schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0 and later.

Schedule Reports

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

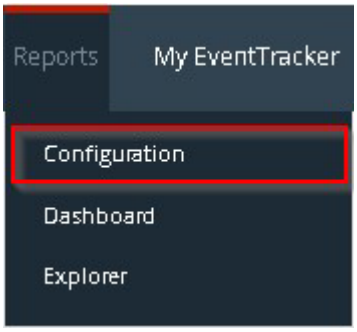


Figure 36

2. Navigate to **Reports>Configuration**.

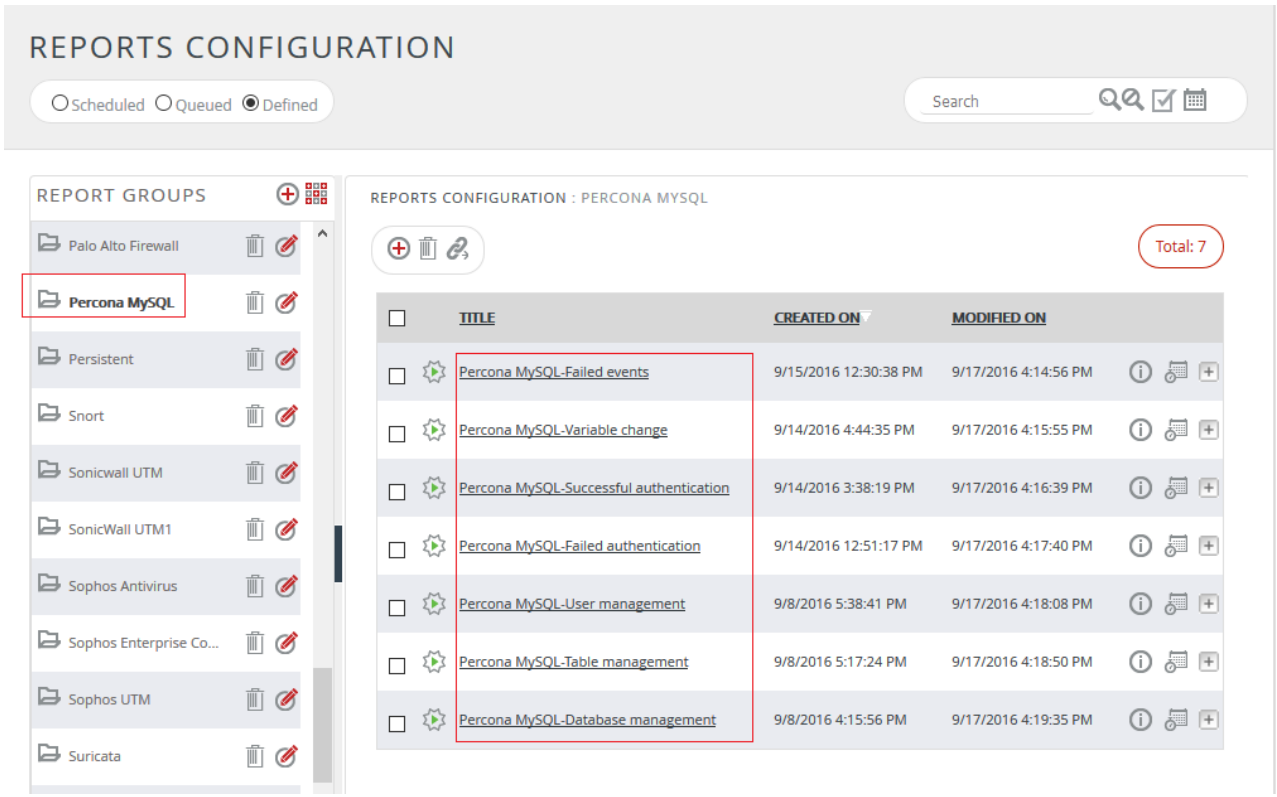


Figure 37

3. Select **Percona MySQL** in report groups. Check **Defined** dialog box.
4. Click on '**schedule**'  to plan a report for later execution.

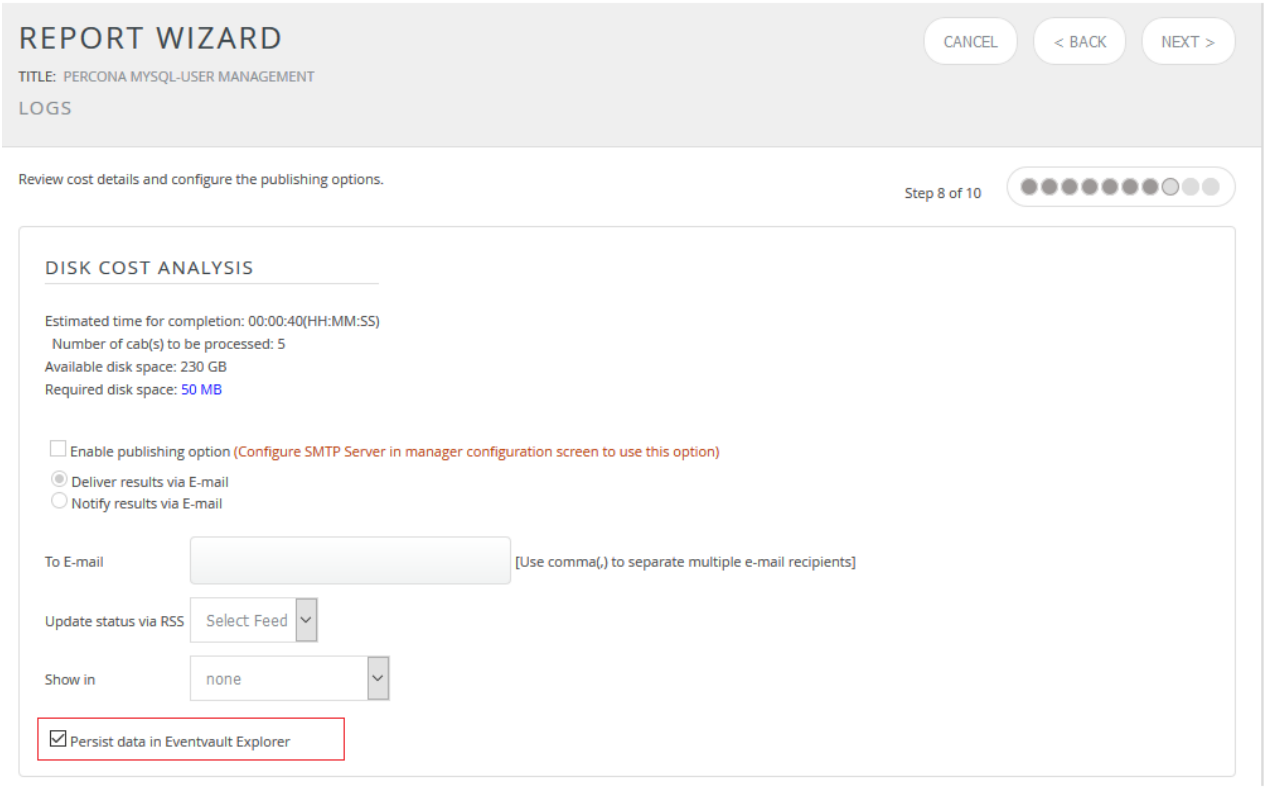

REPORT WIZARD
CANCEL
< BACK
NEXT >
TITLE: PERCONA MYSQL-USER MANAGEMENT
LOGS
Review cost details and configure the publishing options.
Step 8 of 10
DISK COST ANALYSIS
Estimated time for completion: 00:00:40(HH:MM:SS)
Number of cab(s) to be processed: 5
Available disk space: 230 GB
Required disk space: 50 MB
Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)
Deliver results via E-mail
Notify results via E-mail
To E-mail
[Use comma(,) to separate multiple e-mail recipients]
Update status via RSS
Select Feed
Show in
none
Persist data in Eventvault Explorer

Figure 38

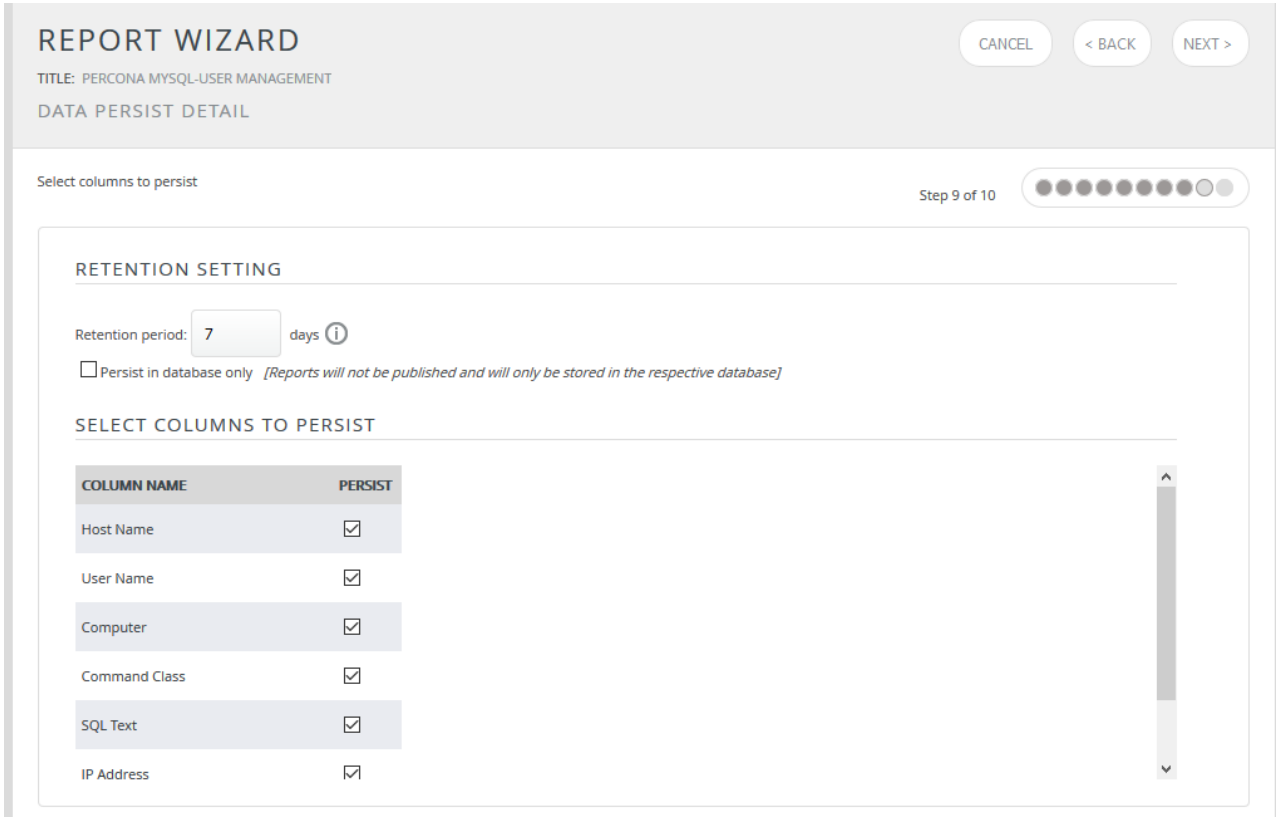


Figure 39

5. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
6. Proceed to next step and click **Schedule** button.
7. Wait till the reports get generated.

Create Dashlets

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

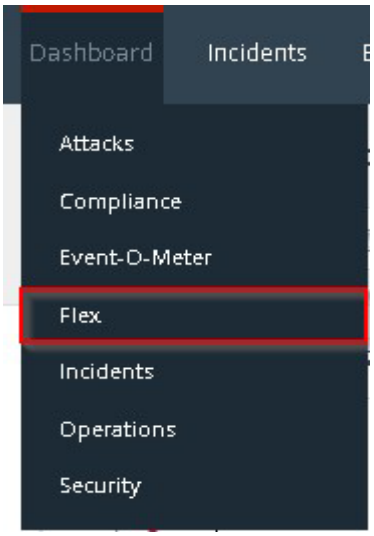


Figure 40

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

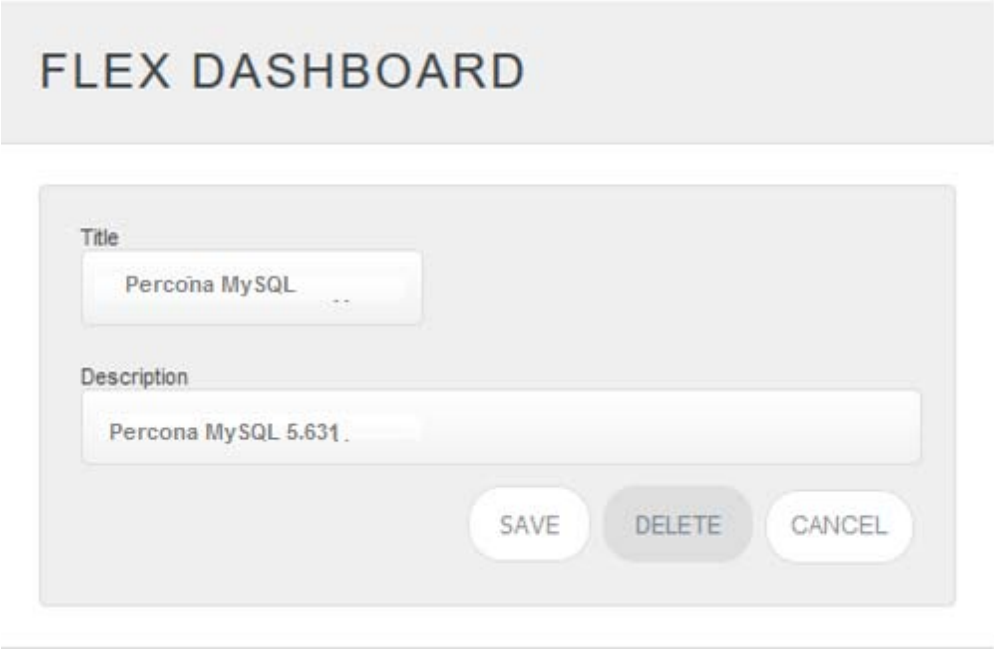


Figure 41

4. Fill suitable title and description and click **Save** button.
5. Click ⚙ to configure a new flex dashlet. Widget configuration pane is shown.

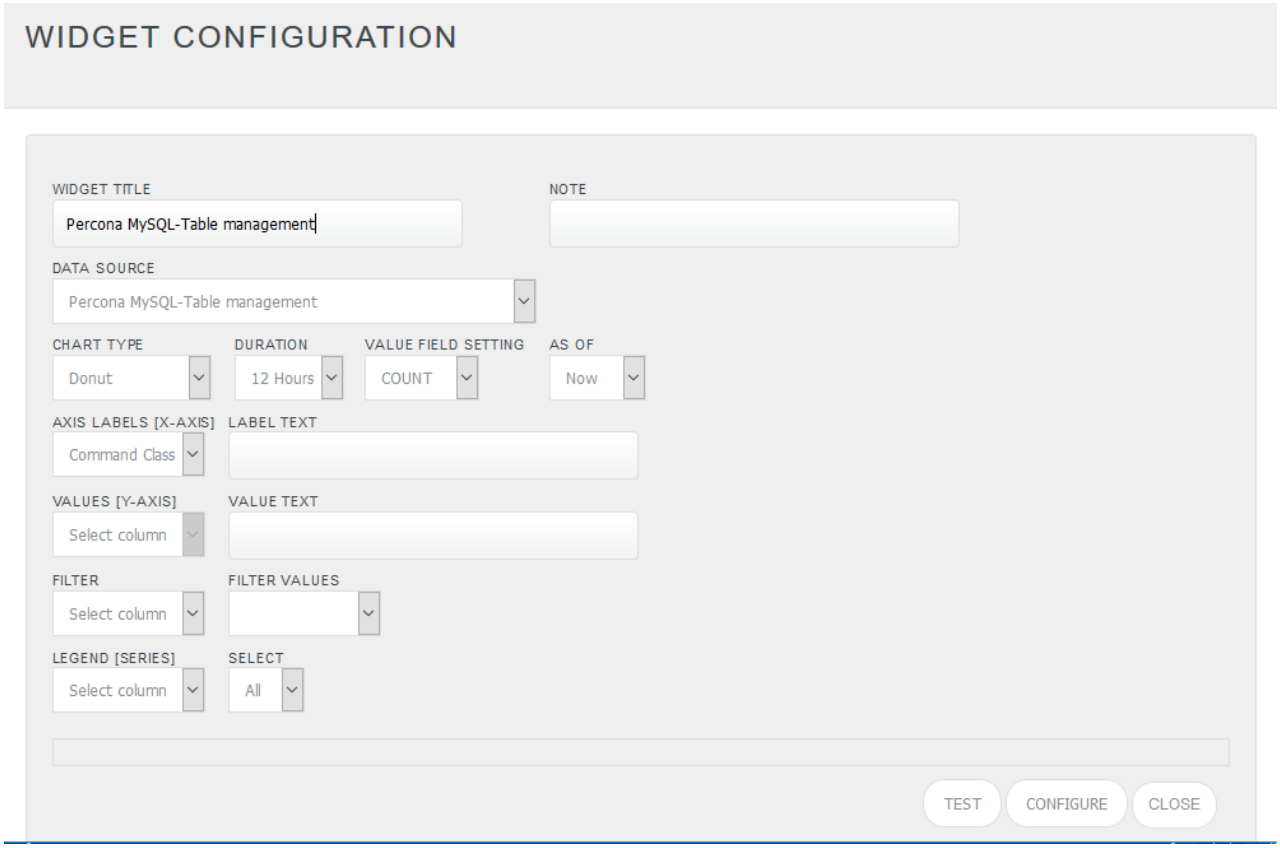


Figure 42

6. Locate earlier scheduled report in **Data Source** dropdown.
7. Select **Chart Type** from dropdown.
8. Select extent of data to be displayed in **Duration** dropdown.
9. Select computation type in **Value Field Setting** dropdown.
10. Select evaluation duration in **As Of** dropdown.
11. Select comparable values in **X Axis** with suitable label.
12. Select numeric values in **Y Axis** with suitable label.
13. Select comparable sequence in **Legend**.
14. Click **Test** button to evaluate. Evaluated chart is shown.

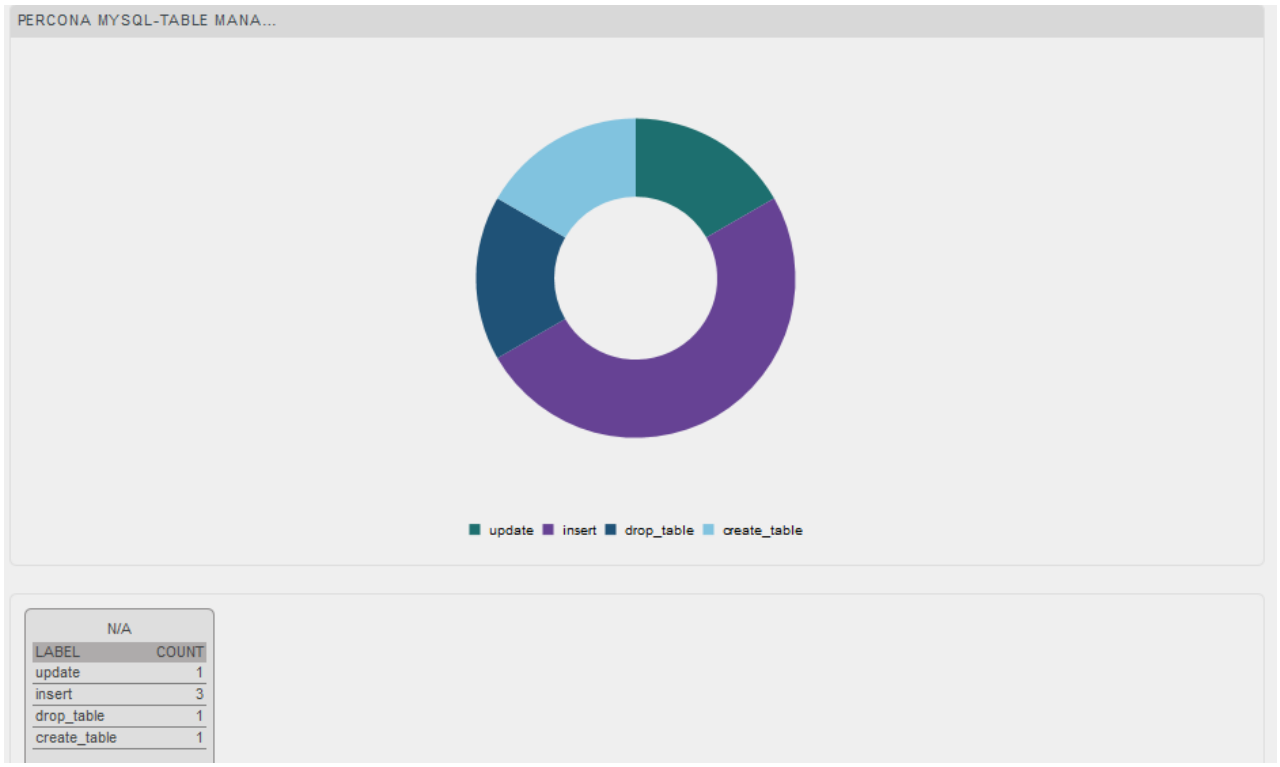


Figure 43

15. If satisfied, click **Configure** button

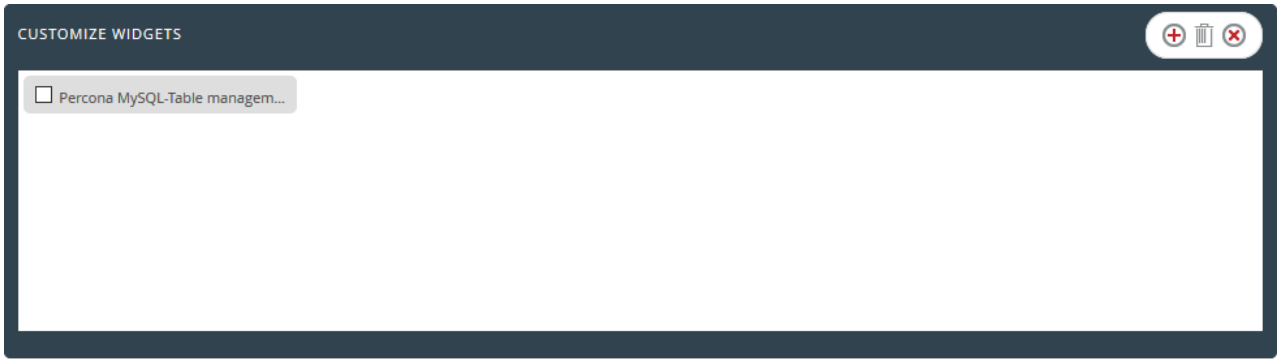


Figure 44

16. Click 'customize' to locate and choose created dashlet.
17. Click to add dashlet to earlier created dashboard.

Sample Dashboards

For below dashboard **DATA SOURCE: Percona MySQL-Table management**

- **WIDGET TITLE:** Percona MySQL-Table management
  CHART TYPE: Donut
  AXIS LABELS [X-AXIS]: Command class

1. Percona MySQL-Table management

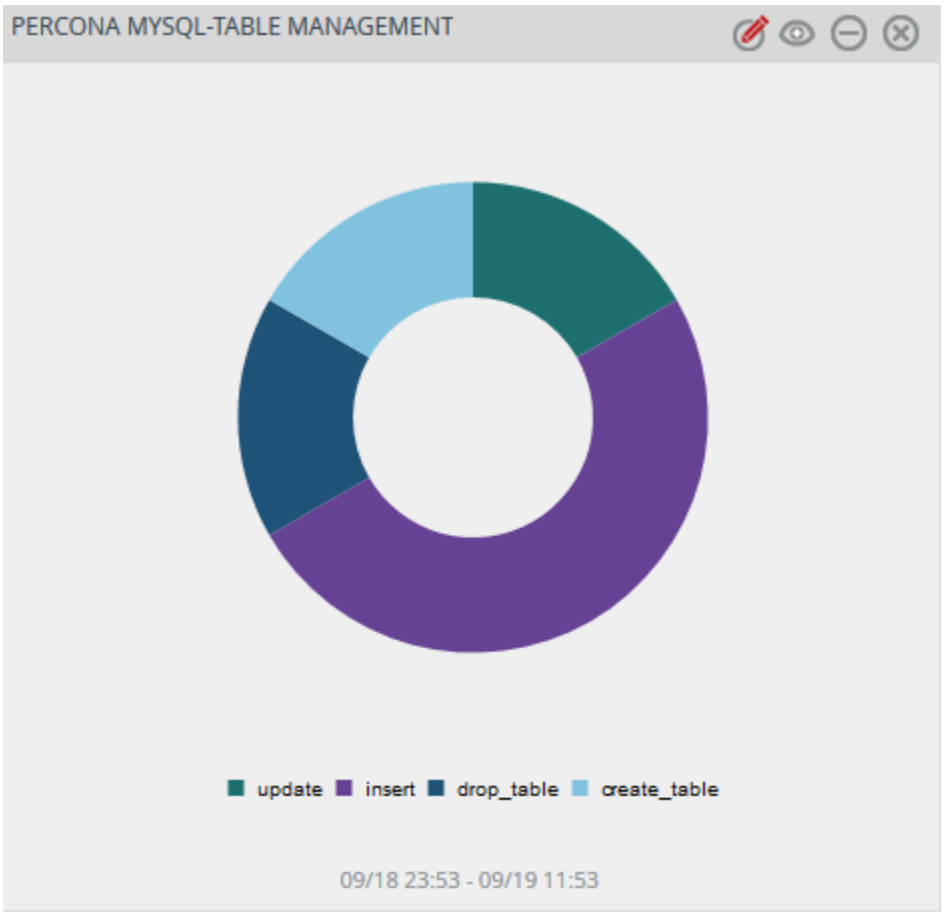


Figure 45