

## Integrate Percona MySQL

## EventTracker Enterprise

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

Publication Date: Oct. 5, 2016

## 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.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



## Table of Contents

About this Guide
Scope
Audience1
Introduction
Pre-requisites
Configuration
AUDIT CONFIGURATION
SYSLOG CONFIGURATION
EventTracker Knowledge Pack7
Categories7
Alerts
Reports
Importing Percona MySQL knowledge pack into EventTracker13
Category14
Alerts16
Parsing Rules
Flex Reports
Knowledge Object
Verifying Percona MySQL knowledge pack in EventTracker21
Categories21
Alerts21
Tokens22
Reports
Knowledge Object
Create Flex Dashboards in EventTracker
Schedule Reports
Create Dashlets
Sample Dashboards



## Introduction

Percona MySQL is an open source software company specializing in <u>MySQL</u> 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:



EventTracker: Integrate Percona MySQL

+	-+	-+	-+
-++   Name   License	Status	Туре	Library
+    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 audit_log_buffer_size audit_log_file og	Value 1048576 /var/log/mysql/audit.l
audit log fluch	OFF
audit_log_format	OLD
audit_log_handler	FILE
audit_log_policy	ALL
audit_log_rotate_on_s	ize 1073741824
audit_log_rotations	10
audit_log_strategy	ASYNCHRONOUS
audit_log_syslog_facil	ity LOG_USER
audit_log_syslog_iden audit	t percona-
audit_log_syslog_prior	rity 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.



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.



```
# Save news errors of level crit and higher in a special file.
                                                     /var/log/spooler
uucp,news.crit
Save boot messages also to boot.log
local7.*
                                                     /var/log/boot.log
# ### begin forwarding rule ###
The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionResumeRetryCount -1
                            # infinite retries if host is down
remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
*.* @192.168.1.129:514
# ### end of the forwarding rule ###
-- INSERT --
```

```
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

				Command			
LogTime	Host Name	User Name	Computer	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

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
9/19/2016 11:46:31 AM	8	PNPL-4-KP / <u>192.168</u>	N/A	N/A	SYSLOG user
Event Type: Information Log Type: Application Category Id: 6	Descriptic Sep 19 NAME= RECORI TIMEST COMM. CONNE STATUS SQLTEX USER=" HOST=" OS_USE IP="" DB="II" />	pn: 11:46:31 192.168.1.119 Sep 19 02 "Query" D="90_1970-01-01T00:00:00" AMP="2016-09-19T06:16:32 UTC" AND_CLASS="drop_table" CTION_ID="9" ="0" T="drop table studentlist" root[root] @ localhost []" localhost" :R=""	2:16:32 localhost pe ,	rcona-audit: <audit_recori< td=""><td>D</td></audit_recori<>	D

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 WKST	N-01 ronaldino	192.168.1.119-SYSLOG	192.168.1.129	TEST	root
SAMPLE LOG			Figure 5			
	EVENT ID	SITE / COMPUTER	USER	DOMAIN		SOURCE
9/19/2016 11:39:18 AM	M <u>8</u>	PNPL-4-KP / 192.168	N/A	N/A	S	YSLOG user
Event Type: Information Log Type: Application Category Id: 6	Descriptio Sep 19 1 NAME=" RECORD TIMESTA CONNEC STATUS= USER="r PRIV_US OS_LOG PROXY_! HOST=" IP=""	n: 1:39:18 192.168.1.119 Connect" ="75_1970-01-01T00: MP="2016-09-19T06:1 TION_ID="9" "1045" nichel" ER="root" IN="" USER="" localhost"	9 Sep 19 02:09:19 localhost pe 00:00" 09:19 UTC"	rcona-audit: <aui< td=""><td>DIT_RECORD</td><td></td></aui<>	DIT_RECORD	

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
		F	Figure 7			

#### SAMPLE LOG

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE	
9/19/2016 11:39:18 AM	8	PNPL-4-KP / 192.168	N/A	N/A	SYSLOG user	
Event Type: Information Log Type: Application Category Id: 6	Descript Sep 19 NAME RECOI TIMES CONIN STATU USER- PRIV_I OS_LC PROM HOST- IP=" DB=" />	ion: 911:39:18 192.168.1.119 Sep 1 ="Connect" RD="75_1970-01-01100:00:00" TAMP="2016-09-19706:09:19 ( IECTION_ID="9" ="christy" USER="root" SGIN=" Y_USER=" ="Tocalhost"	19 02:09:19 localih JTC"	ost percona-audit: <audi< td=""><td>T_RECORD</td><td></td></audi<>	T_RECORD	
			Figur	e 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 ( StudentN ame		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 ( ;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		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	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



#### SAMPLE LOG

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
9/19/2016 11:41:11 AM	8	PNPL-4-KP / <u>192.168</u>	N/A	N/A	SYSLOG user
Event Type: Information Log Type: Application Category Id: 6	Description Sep 19 ' NAME=' RECORE TIMEST/ COMMA CONNE( STATUS: SQLTEX USER=''1 HOST='' OS_USE IP='''' DB=''IIT />	n: 11:41:11 192.168.1.119 Sep 19 02 "Query" >="85_1970-01-01T00:00:00" AMP="2016-09-19T06:11:11 UTC" AVD_CLASS="insert" CTION_ID="9" ="0" T="insert into studentlist values(" root[root] @ localhost []" localhost" R=""	2:11:11 localhost pe	rcona-audit: <audit_recori< th=""><th>&gt;</th></audit_recori<>	>
		F	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

				Command			
LogTime	Host Name	User Name	Computer	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
			Elevine 44				

Figure 11



#### SAMPLE REPORT

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
9/17/2016 7:02:38 PM	8	PNPL-4-KP / <u>192.168</u>	N/A	N/A	SYSLOG user
Event Type: Information Log Type: Application Category Id: 6	Descripti Sep 17 NAME- RECOR TIMEST COMM CONNI STATU: SQLTE: USER= HOST= OS_US IP="" DB=""	on: 19:02:38 192.168.1.119 Sep 17 ( ="Query" D="8_1970-01-01T00:00:00" IAMP="2016-09-17T13:32:36 UT0 AND_CLASS="grant" ECTION_ID="2" S="0" KT=GRANT ALL PRIVILEGES ON ' "root[root] @ localhost []" "localhost" ER=""	19:32:36 localhost p -" * . * TO "rachel"@"{{	ercona-audit: <audit_rec< td=""><td>TORD</td></audit_rec<>	TORD

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
I			Figure 13			

#### SAMPLE LOG

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
9/16/2016 3:11:02 PM	8	PNPL-4-KP / <u>192.168</u>	N/A	N/A	SYSLOG user
Event Type: Information Log Type: Application Category Id: 6	Descriptic Sep 16 NAME= RECORI TIMEST. COMM/ CONNE STATUS SQLTES USER=" HOST=" OS_USE IP="192 DB="TE />	Dn: 15:11:02 192.168.1.119 Sep 16 05 "Query" 3="174_1970-01-01T00:00:00" AMP="2016-09-16T09:41:01 UTC" AND_CLASS="set-option" CTION_ID="18" ="0" T="SET NAMES latin1" root[root] @ pnpl-4-kp.toons.local" i;R="" .168.1.129" ST"	5:41:01 localhost pe 1	rcona-audit: <audit_recor< td=""><td>D</td></audit_recor<>	D

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

🖂 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	Descript Sep 16 NAME RECOM TIMES COMM CONN STATU SQLTE USER= HOST: OS_US IP="19 DB="T P>	ion: 15:11:02 192.168.1.119 Sep 1 ="Query" RD="174_1970-01-01T00:00:00 TAMP="2016-09-16T09:41:01 U RMD_CLASS="set-option" ECTION_ID="18" S="0" XT="SET HOST_NAME=192.16 "root(root) @ pnpl-4.kp.toons "pnpl-4.kp.toons.local" IER="" 2.168.1.129" EST"	16 05:41:01 localhi " JTC" :8.1.119" .local [192.168.1.1	ost percona-audit: <audit< td=""><td>_RECORD</td></audit<>	_RECORD

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.

## Category

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



💺 Export Import Utility		_ 🗆 🗙
Export Import		
1. Provide the path and file nar 2. Click the Import button.	ne of the Categories file. Use the '' button to browse and locate the import file.	
<ul> <li>Category</li> </ul>		
C Filters		
C Systems and Groups	Source :	
C RSS Feeds		
C Reports		
C Behavior Rules		
C SCAP		
C Token Value		
	Import	Close

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.







## Alerts

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

🖫 Export Import Utility	×
Export Import	
Export       Import         1. Provide the path and file name of the Alerts file. Use the '' button to browse and locate the import file.         2. Click the Import button.         Options         Category         Filters         Alerts         Systems and Groups         RSS Feeds         Reports         Surce :         *isalt         Token Value	
Import	

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



## **Parsing Rules**

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

🖫 Export Import Utility	
Export Import	
<ol> <li>Provide the path and file name of token value file. Use the '' button to browse and locate the import file.</li> <li>Click the Import button         <ul> <li>Category</li> <li>Filters</li> <li>Alerts</li> <li>Systems and Groups</li> <li>RSS Feeds</li> <li>Reports</li> <li>Behavior Rules</li> <li>SCAP</li> <li>Token Value</li> </ul> </li> </ol>	
Import Clos	e

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.

Export Import Utility	X
Selected token values are imp	ported successfully.
	ОК
Figure 23	



## Flex Reports

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

<ol> <li>Provide the path and file na</li> <li>Click the Import button Note : If report(s) contains ten</li> </ol>	ame of Schedule Report file. Use the '' button to browse and locate the import file. aplate, first import template and proceed with exportimport utility.
Options	Location
Category	
Filters	
Alerts	Legacy (*.issch)
Systems and Groups	Source :
RSS Feeds	*.issch
Reports	
Behavior Rules	
SCAP	
🔘 Token Value	

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.







## Knowledge Object

- 1. Click the Admin menu, and then click Knowledge Objects.
- 2. Click on T 'Import' option.

KNOWLE	DGE	DBJECTS		
	) ] 1			
OnenDNS				
Palo Alto	00		SELECT OBJECT FROM THE LEFT PANEL	
Pulse Secure MAG S	5 🧭 🙁			
RSA SecurID Auther	n 🧭 🙁			
Sharepoint Server	0			
Snort	0			
Sonicwall	0			
SQL Server	0			
Suricata	Ø 🗵			
Symantec EndPoint				
Teradata	0			
Trend micro intersc	. Ø 🗵	=		
Vmware	0			
Windows account m	nana 🔟 (	8		

Figure 26

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

IMPORT	
Select file <b>Browse</b> No file selected.	UPLOAD



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



IMP	ORT		
Select fil	e <b>Browse</b> No file sele	cted.	UPLOAD
	OBJECT NAME	APPLIES TO	
	Percona MySQL	5.6.31	
			MERGE OVERWRITE

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.



CATEGORY MANAGEMENT

# 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.

#### Category Tree Search 🗄 🔁 OKTA SSO Total category groups: 355 Total categories: 3,129 DenDNS Umbrella Insights and Platfo Last 10 modified categories 🗄 🔁 Oracle NAME MODIFIED DATE MODIFIED BY 🗄 🔁 Paloalto 🗟 🔁 Percona MySQL Percona MySQL: User management 9/17/2016 4:05:59 PM ETAdmin 🗉 🗐 Percona MySQL: Database manage Percona MySQL: Table management 9/17/2016 4:05:39 PM ETAdmin Percona MySQL: Table managemen Percona MySQL: Database management 9/17/2016 4:05:24 PM ETAdmin E Percona MySQL: User authenticatio E Percona MySQL: User authenticatio 9/17/2016 4:03:45 PM Percona MySQL: Variable change ETAdmin Percona MySQL: User management ETAdmin Percona MySQL: User authentication successful 9/17/2016 3:57:27 PM E Percona MySQL: Variable change FTAdmin 9/17/2016 3:56:48 PM Percona MySQL: User authentication failed 🗐 🔁 Raritan Commandcenter secure gatewa ETAdmin Kaspersky Endpoint Security: Device control 8/30/2016 12:06:13 PM 🗄 🗔 RSA SecuriD 🖶 🔁 Ruckus Wireless ZoneDirector 8/16/2016 5:58:16 PM SEP: Administrator account unlocked ETAdmin 🗄 🔁 Snort 8/16/2016 4:49:28 PM SEP: Virus detected ETAdmin 🗄 🗔 Solaris BSM ETAdmin SEP: Application blocked 8/16/2016 3:36:57 PM 🗄 🔁 Sonicwall UTM 🗄 🔁 Sophos Enterprise Console 🗄 🔁 Sophos UTM

### 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.



ALERT MANAGEMEN	Т					Search I	Alert n	ame 🗸	percona	୍ର୍ୟ
ACTIVATE NOW Click 'Activate	t <b>e Now'</b> after ma	king all cha	anges						Total: 1	Page Size 25 🗸
	THREAT	<u>ACTIVE</u>	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
Percona MySQL: User management	High									5.6.31
DELETE										

#### Figure 31

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

	×
Successfully saved co	figuration.
	ОК
	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.



PARSING R	ULE					
Parsing Rule Ten Palo Alto Firewall	nplate			Group	Percona MySQL	2
Percona MySQL	Ū Ø	Token-Value Display name		_ \ \ \	CERARATOR	-
Snort IDS		DISPLAY NAME	COMMAND_CLASS=	1AG	"	"
Sonicwall UTM	Ŵ Ø	+ Database	DR-			
Sophos Antivirus	Ū Ø		-0U			
Sophos Enterprise Co Suricata		🕂 🗌 Host Name	HOST=			п
Symantec Endpoint Pr	Ē Ø	+ 🗌 IP Address	IP=			п У
Syslog	Ü 🏈		ADD RULE EDIT	DELETE MOVE TO G	ROUP	V-VALUE WIZARD
Syslog login failure	Ū Ø					
Trend Micro InterSca						
menu Micro muersca						



## 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**.



REPORTS CONFIGURATION							
O Scheduled O Queued	Oefined		Search	QQ 🗹 🗎			
REPORT GROUPS	$\oplus$	REPORTS	CONFIGURATION : PERCONA MYSQL				
Palo Alto Firewall	Ū 🖉 î	<b>Ð</b> 🗓	Ø,			Total: 7	
Percona MySQL	Ū Ø		mle	CREATED ON	MODIFIED ON		
Persistent	11 🧭		Percona MySQL-Failed events	9/15/2016 12:30:38 PM	9/17/2016 4:14:56 PM	() 🖉 🕂	
Snort	1		Percona MySQL-Variable change	9/14/2016 4:44:35 PM	9/17/2016 4:15:55 PM	() 🎜 🗉	
Sonicwall UTM	Ü 🏉		Percona MySQL-Successful authentication	9/14/2016 3:38:19 PM	9/17/2016 4:16:39 PM	() 🎘 Ŧ	
SonicWall UTM1	Ü 🧭		Percona MySQL-Failed authentication	9/14/2016 12:51:17 PM	9/17/2016 4:17:40 PM	() 🖉 Ŧ	
Sophos Antivirus	Ü Ø		Percona MySQL-User management	9/8/2016 5:38:41 PM	9/17/2016 4:18:08 PM	() 🖉 🗉	
Sophos Enterprise Co	Ü 🧭		Percona MySQL-Table management	9/8/2016 5:17:24 PM	9/17/2016 4:18:50 PM	() 🖉 Ŧ	
Sophos UTM	1		Percona MySQL-Database management	9/8/2016 4:15:56 PM	9/17/2016 4:19:35 PM	() 🖉 🗉	
🔁 Suricata	1						



## 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.



KNOWLE	EDGE	OB	JECTS						
DBJECTS Jumper OS	e I I e Ø8	A A	DBJECT NAME Percona MySC NPPLIES TO 5.6.31 ULES THT F		EVENT SOURCE	EVENT ID	EVENT TYPE	1	<b>+</b>
LOGbinder SP						CIENTID			
Logbinder SQL	Ø	Ŀ	+ PERCONA-All events	Application	SYSLOG user		Information		
McAfee EPO	Ø		MESSAGE SIGNATURE:	(SQLTEXT\=\".*\")					
Mcafee Firewall VP	PN 🏈 🗵		MESSAGE EXCEPTION						
McAfee Intrushield	d IØ								
McAfee VirusScan	E 🧭 🙁		EXPRESSIONS						
OKTA SSO	<b>8</b>					51000			
OpenDNS	<b>8</b>		EXPRESSION TYPE	'E FORMAI STRING	EXPRESSION 1	EXPRE	SSION 2		
Palo Alto	0		Key Value Delimite	er	=	١n		$\overline{\mathbf{A}}$	
Percona MySQL	Ø8								
Pulse Secure MAG	s@ 🙁								
RSA SecurID Authe	en 🧭 🙁								
Sharapoint Sequer	Ø								

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.







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

### REPORTS CONFIGURATION

O Scheduled O Queued	Defined				Search	2 <b>Q</b> 🗹 🗎
REPORT GROUPS	$\oplus$	REPORTS	CONFIGURATION : PERCONA MYSQL			
Palo Alto Firewall	Ū 🖉 î	<b>⊕</b> ∎	Ĉ,			Total: 7
Percona MySQL	1		IIILE	CREATED ON	MODIFIED ON	
Persistent	1		Percona MySQL-Failed events	9/15/2016 12:30:38 PM	9/17/2016 4:14:56 PM	() 🖉 Ŧ
Snort	Ū Ø		Percona MySQL-Variable change	9/14/2016 4:44:35 PM	9/17/2016 4:15:55 PM	i 🖉 🗉
Sonicwall UTM	Ū Ø		Percona MySQL-Successful authentication	9/14/2016 3:38:19 PM	9/17/2016 4:16:39 PM	() 🖉 🗉
SonicWall UTM1	Ū Ø		Percona MySQL-Failed authentication	9/14/2016 12:51:17 PM	9/17/2016 4:17:40 PM	() 🖉 Ŧ
Sophos Antivirus	1		Percona MySQL-User management	9/8/2016 5:38:41 PM	9/17/2016 4:18:08 PM	() 🖉 Ŧ
Sophos Enterprise Co	1		Percona MySQL-Table management	9/8/2016 5:17:24 PM	9/17/2016 4:18:50 PM	() 🖉 Ŧ
Sophos UTM	1		Percona MySQL-Database management	9/8/2016 4:15:56 PM	9/17/2016 4:19:35 PM	i 🖉 🗉
🔁 Suricata	1			1		

#### Figure 37

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



REPORT WIZA	ARD MANAGEMENT		CANCEL < BACK NEXT >
Review cost details and configu	re the publishing options.		Step 8 of 10
DISK COST ANALY Estimated time for complet Number of cab(s) to be pro Available disk space: 230 Gl Required disk space: 50 ME Enable publishing option Deliver results via E-mai Notify results via E-mai	/SIS tion: 00:00:40(HH:MM:SS) occessed: 5 B 3 on (Configure SMTP Server in m ail	nager configuration screen to use this option)	
To E-mail		[Use comma(,) to separate multiple e-mail recipients]	
Update status via RSS Se	elect Feed 🗸		
Show in no	one 🗸		
Persist data in Eventva	ult Explorer		

Figure 38



REPORT W TITLE: PERCONA MYSQL-U DATA PERSIST DE	IZARD ISER MANAGEMENT TAIL	CANCEL < BACK NEXT >
Select columns to persist		Step 9 of 10
RETENTION S Retention period: Persist in databa	ETTING 7 days (j) se only <i>[Reports will not be pu</i> MNS TO PERSIST	ublished and will only be stored in the respective database]
COLUMN NAME	PERSIST	^
Host Name		
User Name		
Computer		
Command Class		
SQL Text		
IP Address		v

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.



Dashboard	Incidents E						
Attacks							
Complian	Compliance						
Event-O-N	leter						
Flex							
Incidents							
Operation	Operations						
Security							
	· ·						

Figure 40

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

Title	
Percona MySQL	
Description	
Percona MySQL 5.631.	

#### 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.



### WIDGET CONFIGURATION

WIDGET TITLE			NOTE		
Percona MySQL-Table	management				
DATA SOURCE Percona MySQL-Table	management		~		
CHART TYPE	DURATION 12 Hours ~	COUNT	NG AS OF	~	
AXIS LABELS [X-AXIS] Command Class	LABEL TEXT				
VALUES [Y-AXIS] Select column	VALUE TEXT				
FILTER Select column	FILTER VALUES	~			
LEGEND [SERIES] Select column	All V				

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.



PERCONA MYSQL-TABLE MANA	
N/A LABEL COUNT update 1 insert 3 drop_table 1	update insert drop_table create_table

Figure 43

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

CUSTOMIZE WIDGETS	⊕ <u>∎</u> ⊗
Percona MySQL-Table managem	



- 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

