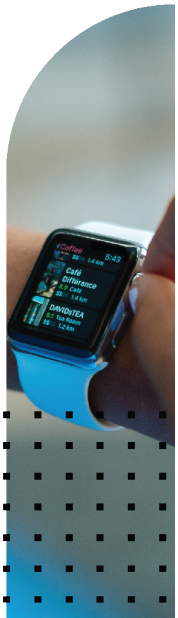
SQL Log Database Query

FortiAnalyzer 7.0.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

November 14, 2022
FortiAnalyzer 7.0.0 SQL Log Database Query
02-700-730856-20221114

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-07-14	Initial release.
2022-11-14	Updated Creating datasets on page 6.

Introduction

This document describes how to write your own SQL query statements to create custom datasets.

FortiAnalyzer supports local PostgreSQL databases for the storage of log tables.

For additional information about the FortiAnalyzer dataset, see the FortiAnalyzer Administration Guide on the Fortinet Docs Library.

To create a report based on log messages in the local database, you can use either the predefined datasets or create your own custom dataset by querying the log message in the SQL database on the FortiAnalyzer.

Creating datasets

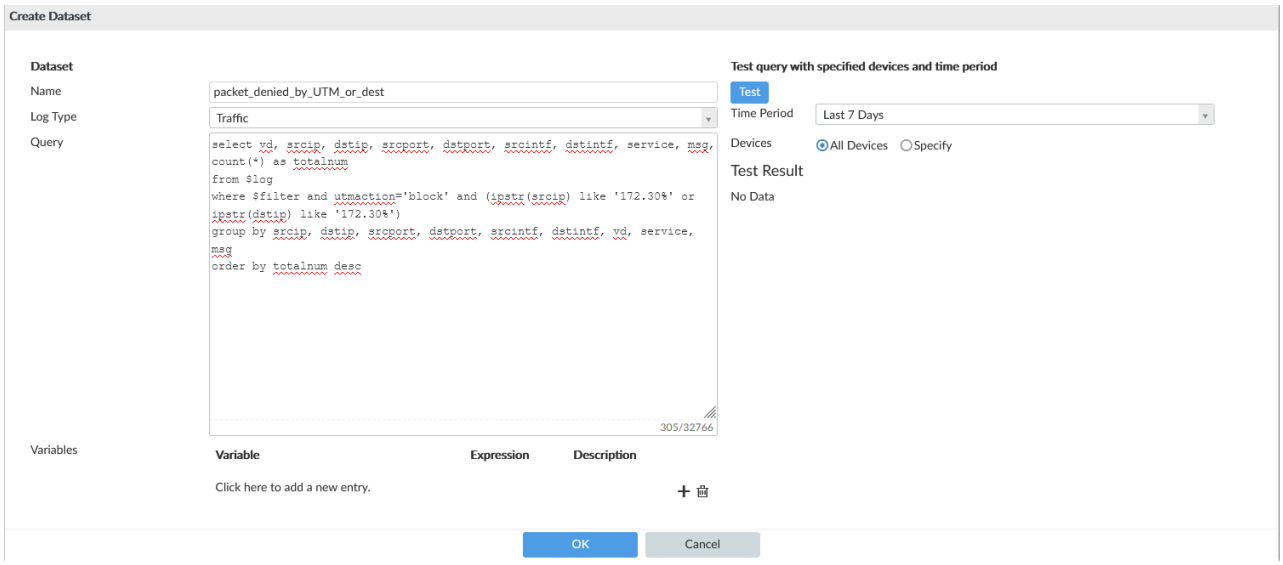
The following procedure describes how to create datasets in FortiAnalyzer.

Datasets define what data is extracted from the database and represented in a report's chart. While FortiAnalyzer does provide pre-defined datasets that address the most common queries, you need to understand Structured Query Language, also known as SQL, in order to modify those datasets or create your own.

For additional details, see the *FortiAnalyzer Administration Guide* and *FortiAnalyzer CLI Reference* in the Fortinet Docs Library.

To create a custom dataset:

1. Go to *Reports* > *Report Definitions* > *Datasets*.
2. Click *Create New*.
3. Provide the required information for the new dataset.



Name	Enter a name for the dataset.
Log Type	Select the log type to be used in the dataset. `$log` is used in the SQL query to represent the log type you select, and it is run against all tables of this type.
Query	Enter the SQL query used for the dataset. An easy way to build a custom query is to copy and modify a predefined dataset's query.
Variables	Click the *Add* button to add variable, expression, and description information.

	If added, the expression for the variable will be used when configuring filters for reports that use this dataset. For example, if *Variable* = *User (user)* and *Expression* = *coalesce(nullifna(`user`), ipstr(`srcip`))*, then the expression will be used when *User (user)* is selected as the *Log Field* in a report's filter. See Filtering report output in the *FortiAnalyzer Administration Guide*.
Test query with specified devices and time period Device and time filters are applied by $filter in the dataset.	
Test	Click to test whether or not the SQL query is successful.
Time Period	Use the dropdown list to select a time period. When selecting *Custom*, enter the start date and time, and the end date and time.
Devices	Select *All Devices* or *Specify* to select specific devices to run the SQL query against. Click the *Select Device* button to add multiple devices to the query.

4. Click *OK*.
   Once a dataset has been configured, it can be used to configure charts which can be added to reports.

To add a dataset to a chart:

1. Go to *Reports* > *Report Definitions* > *Chart Library*, and click *Create New* or edit an existing chart.
2. Select your custom dataset from the *Dataset* dropdown, configure the chart details, and click *OK*.

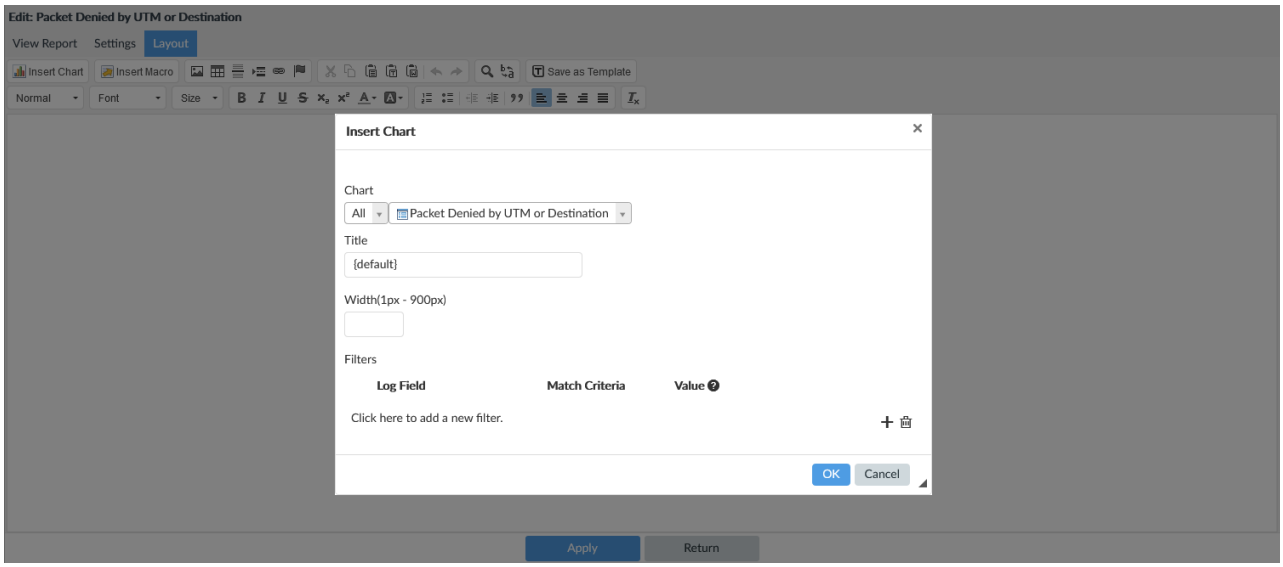
   The chart based on your custom dataset is now available for use in reports.|

The SQL dataset test function can be used to determine if any errors are present in the SQL format. It should not be used to test returned values as those may be different than the ones used in reports.

To use a chart in reports:

1. Go to *Reports* > *Report Definitions* > *All Reports*, right-click and select *Create New*.
2. Enter a name for the report, select a template and a save location, and click *OK*.

3. On the *Layout* tab, click *Insert Chart*, select your custom chart from the *Chart* dropdown, and click *OK*.



4. Configure the remaining report settings, and save your changes.

For more information, see Creating Charts and Creating Reports in the *FortiAnalyzer Administration Guide*.

Testing datasets queries

Once a dataset has been created, you can test the dataset query to confirm it works as intended.

To test a dataset query:

1. Follow the procedures in Creating datasets on page 6, or select an existing dataset.
2. Configure the specified devices and time period as desired.
3. Click *Test*.
   The query results are displayed. If the query is not succesful, an error message appears in the *Test Result* pane. See Troubleshooting SQL test queries on page 8.
4. Click *OK*.

Troubleshooting SQL test queries

If the SQL test is unsuccessful, an error message appears in the results pane indicating the cause of the problem.

Following are some example error messages and possible causes:

```
ERROR: syntax error at or near...
```

- Check that SQL keywords are spelled correctly, and that the query is well-formed.
- Table and column names are demarked by grave accent (`) characters. Single (') and double (") quotation marks will cause an error.

```
No Data
```

- The query is correctly formed, but no data has been logged for the specified log type. Check that you have configured and authorized a logging device of that type on the FortiAnalyzer.

SQL tables

SQL is the database language that FortiAnalyzer uses for logging and reporting. Log data is inserted into the SQL database for log view and report generation. FortiAnalyzer uses a PostgreSQL database.

In an SQL database all information is represented as tables, and each table consists of a set of rows and columns. There are two types of tables:

- User tables, which contain information that is in the database, and
- System tables, which contain the database description.

You can use information from SQL tables to create custom datasets for use in report charts.

Log types and subtypes

Log types each have a SQL table that can be specified when creating datasets.

Log types also include log sub-types, which are types of log messages that are within the main log type.

For more information on log types and subtypes, see the FortiAnalyzer and FortiGate *Log Message Reference* guides on the Fortinet Document Library.

Log types available in FortiAnalyzer datasets

Source	Log type
FortiGate	Appevent
	Intrusion Prevention
	Content Log
	Data Leak Prevention
	DNS
	Email Filter
	Event
	FortiClient System Event
	FortiClient Security Event
	FortiClient Traffic
	File Filter
	GTP
	Vulnerability Scan
	Protocol
	SSH
	SSL
	Traffic
	Virus
	VoIP
	Web Application Firewall
	Web Filter
	Local Event
FortiMail	Email Filter
	Event
	History
	Virus

Source	Log type
FortiAnalyzer	Appevent
	Event
	Local Event
FortiWeb	Intrusion Prevention
	Event
	Traffic
FortiCache	Appevent
	Intrusion Prevention
	Content Log
	Data Leak Prevention
	Email Filter
	Event
	Vulnerability Scan
	Traffic
	Virus
	VoIP
	Web Filter
FortiClient	FortiClient System Event
	FortiClient Security Event
	FortiClient Traffic
Syslog	Generic
FortiManager	Appevent
	Event
FortiSandbox	Event
	Vulnerability Scan
	Virus
FortiDDoS	Intrusion Prevention
	Event
FortiAuthenticator	Event

Source	Log type
FortiProxy	Appevent
	Intrusion Prevention
	Content Log
	Data Leak Prevention
	DNS
	Email Filter
	Event
	File Filter
	Vulnerability Scan
	Protocol
	SSH
	SSL
	Traffic
	Virus
	VoIP
	Web Filter
FortiNAC	Asset
	Event
FortiFirewall	DNS
	Event
	File Filter
	GTP
	SSH
	SSL
	Traffic
FortiDeceptor	Event
Fabric	Normalized

Log severity levels

Each log entry contains a level field that indicates the estimated severity of the event that caused the log entry. When a logging severity level is defined, the FortiAnalyzer unit logs all messages at and above the selected severity level. For example, if you select Error, FortiAnalyzer logs Error, Critical, Alert, and Emergency level messages.

The Debug log severity level is rarely used. Debug log messages are useful when the FortiAnalyzer unit is not functioning properly. Debug log messages are only generated if the log severity level is set to Debug. Debug log messages are generated by all subtypes of the event log.

To view information about log severity levels, see the *FortiAnalyzer Log Message Reference*.

Log fields

Each log table stored in an SQL database contains log fields that can be used in datasets.

You can view a full list of the fields available for each log type in the *FortiAnalyzer Postgres Schema* file available from the FortiCloud Support page.

Examples of custom datasets

The following examples illustrate how to write custom datasets.

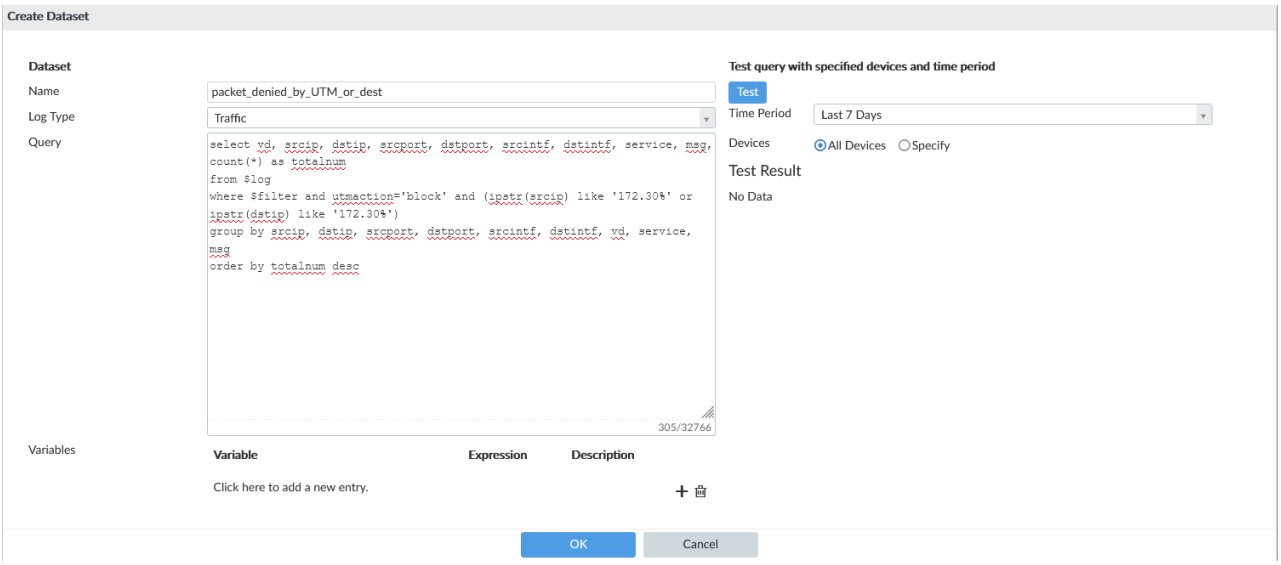
After you create the datasets, you can use them when you configure chart templates under *Reports* > *Report Definitions* > *Chart Library*. Configured charts can be selected when creating or modifying reports.

For more information on creating charts and reports, see the FortiAnalyzer Administration Guide.

Example 1: Packets denied by UTM for a source or destination matching '172.30.xx.xx':

1. Go to *Reports* > *Report Definitions* > *Datasets*, and click *Create New*.
2. Enter a name for the dataset, for example: *packet_denied_by_UTM_or_dest*.
3. Under *Log Type*, select *Traffic*.
4. Configure *Time Period* and *Devices*.
5. Under *Query*, enter the following:

```
select vd, srcip, dstip, srcport, dstport, srcintf, dstintf, service, msg, count(*) as
     totalnum
from $log
where $filter and utmaction='block' and (ipstr(srcip) like '172.30%' or ipstr(dstip)
     like '172.30%')
group by srcip, dstip, srcport, dstport, srcintf, dstintf, vd, service, msg
order by totalnum desc
```

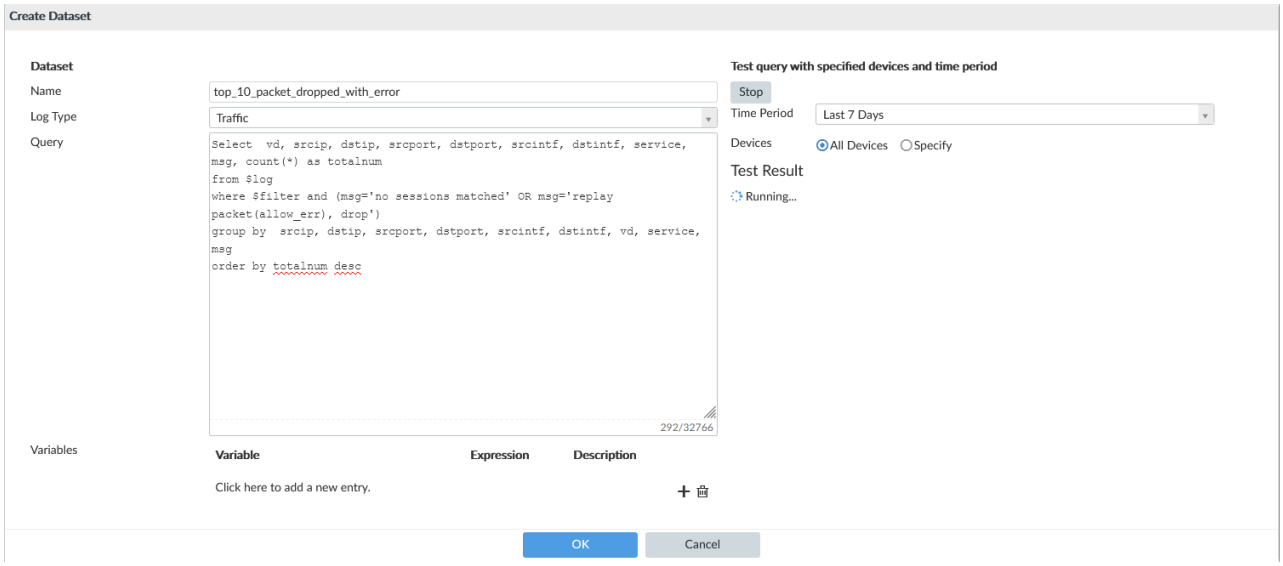


Example 2: Top 10 hosts that had the most packets dropped with error message 'no session matched' or 'replay packet(allow_err), drop':

1. Go to *Reports* > *Report Definitions* > *Datasets*, and click *Create New*.
2. Enter a name for the dataset, for example: *top_10_packet_dropped_with_error*.
3. Under *Log Type*, select *Traffic*.
4. Configure *Time Period* and *Devices*.

5. Under *Query*, enter the following:

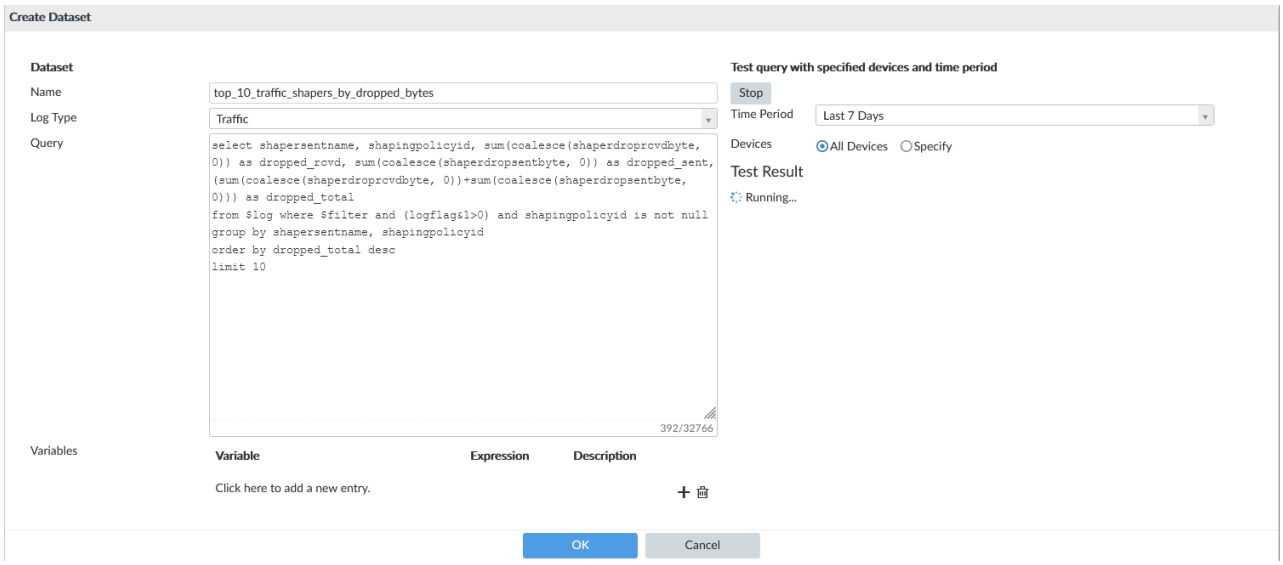
```
Select vd, srcip, dstip, srcport, dstport, srcintf, dstintf, service, msg, count(*) as
     totalnum
from $log
where $filter and (msg='no sessions matched' OR msg='replay packet(allow_err), drop')
group by srcip, dstip, srcport, dstport, srcintf, dstintf, vd, service, msg
order by totalnum desc
```



Example 3: Top 10 traffic shapers by dropped bytes

1. Go to *Reports* > *Report Definitions* > *Datasets*, and click *Create New*.
2. Enter a name for the dataset, for example: *top_10_traffic_shapers_by_dropped_bytes*.
3. Under *Log Type*, select *Traffic*.
4. Configure *Time Period* and *Devices*.
5. Under *Query*, enter the following:

```
select shapersentname, shapingpolicyid, sum(coalesce(shaperdroprcvdbyte, 0)) as
     dropped_rcvd, sum(coalesce(shaperdropsentbyte, 0)) as dropped_sent, (sum
     (coalesce(shaperdroprcvdbyte, 0))+sum(coalesce(shaperdropsentbyte, 0))) as
     dropped_total
from $log where $filter and (logflag&1>0) and shapingpolicyid is not null
group by shapersentname, shapingpolicyid
order by dropped_total desc
limit 10
```


Create Dataset
Dataset
Name
top_10_traffic_shapers_by_dropped_bytes
Log Type
Traffic
Query
select shapersentname, shapingpolicyid, sum(coalesce(shaperdroprcvdbyte, 0)) as dropped_rcvd, sum(coalesce(shaperdropsentbyte, 0)) as dropped_sent, (sum(coalesce(shaperdroprcvdbyte, 0))+sum(coalesce(shaperdropsentbyte, 0))) as dropped_total
from $log where $filter and (logflag&1>0) and shapingpolicyid is not null group by shapersentname, shapingpolicyid
order by dropped_total desc
limit 10
392/32766
Variables
Variable
Expression
Description
Click here to add a new entry.
Test query with specified devices and time period
Stop
Time Period
Last 7 Days
Devices
All Devices
Specify
Test Result
Running...
OK
Cancel

www.fortinet.com