



STORMSHIELD

TECHNICAL NOTE

Stormshield Network
Multifunction Firewall

Using Virtual Log Appliance for Stormshield

Document version: 1.0

Reference: smentno_virtual-log-appliance-v1.2



CONTENTS

REQUIREMENTS	3
FIRST STEPS	3
Access to the server	3
Getting acquainted with the dashboard	4
Initial search	5
QUERY / FILTERING	5
Queries	5
Simple queries	5
Multiple queries	6
Colors and legends	7
Filters	8
Time filter	8
Customized filter	9
ROWS AND PANELS	10
Rows	10
Adding a row	10
Managing rows	10
Panels	11
Adding panels	11
Editing a row	12
Moving or deleting panels	13
Moving or deleting a row	13
MANAGING DASHBOARDS	14
Saving a dashboard	14
Opening a dashboard	14
Sharing a dashboard	15
Saving a static dashboard	15
Extracting a dashboard	15
Automatically refreshing a dashboard	16

REQUIREMENTS

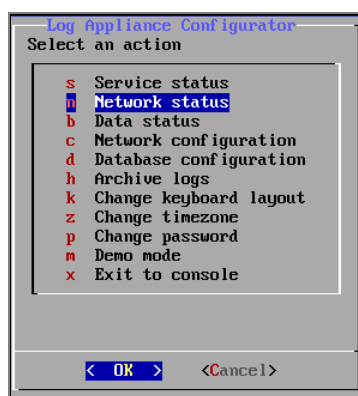
Details on installing the Virtual Log Appliance server for Stormshield are given in the installation guide, available in your secure-access area (<https://mystormshield.eu>).

FIRST STEPS

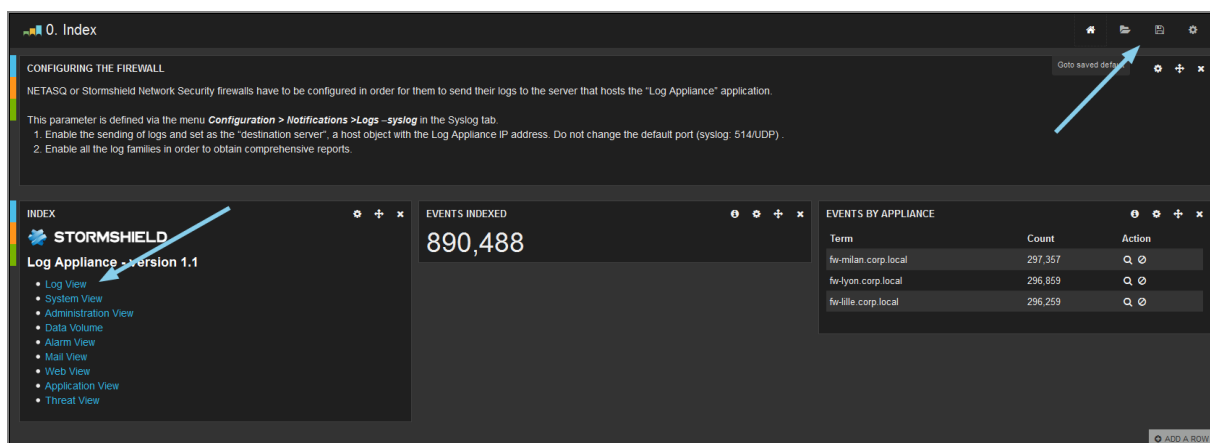
Virtual Log Appliance enables analyzing and searching for events in the form of dashboards, which are available in HTTPS from your browser.

Access to the server





To find out the Virtual Log Appliance server's IP address, start the virtual machine and log on using the default user account ("log") via the console on the hypervisor. Select the entry **Network Status** from the menu **Virtual Log Appliance Configurator**:



Next, log on in HTTPS to the address indicated (authentication with the "log" account necessary) in order to display the homepage (**0. Index**):



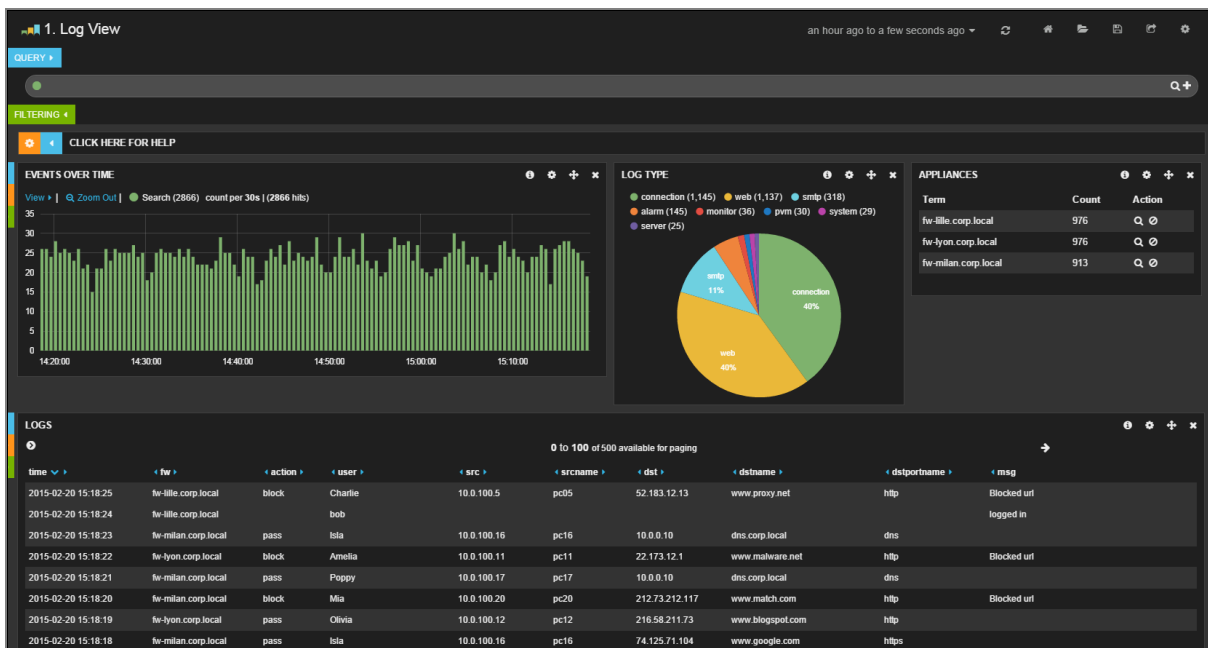
On this page, several panels will appear:

- **0. Index:** contains several icons:
 - : go back to main page
 - : open a view saved earlier
 - : save the current dashboard
 - : settings of the current page

- **Configuring the firewall:** panel reminding you that your Stormshield appliances have to transmit their events in syslog to the server that hosts Log Appliance,
- **Index:** a list of default views (dashboards) has been created for viewing and analyzing logs by category,
- **Events indexed:** current amount of logs received by Log Appliance,
- **Events by appliance:** list of appliances that have already transmitted logs to the Virtual Log Appliance server. For each appliance, a counter indicates the amount of logs sent. The possible actions allow filtering the firewall in question (magnifying glass icon) or removing it from a filter (delete icon).

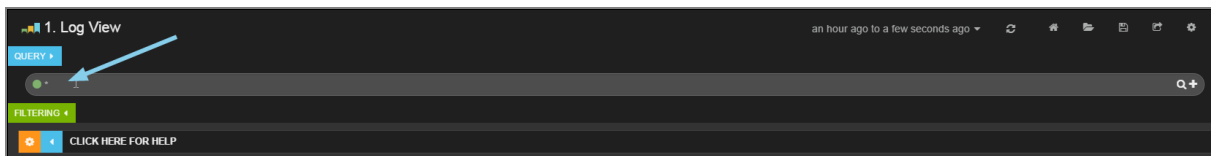
Getting acquainted with the dashboard

In the **Index** panel, click on **Log View** to get your first view. The main role of this view is to perform searches in log files sent by your Stormshield appliances and stored in a database.



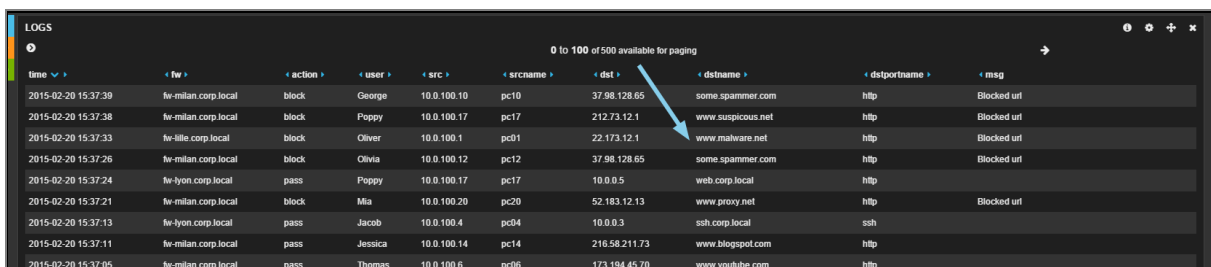
Initial search

Virtual Log Appliance allows searching in databases by following Apache Lucene syntax. Queries have to be entered in the **Query** field located at the top of the page:



Enter your search terms in the **Query** field. The various panels will refresh according to the search performed.

Example
http ssh alarm system



time	fw	action	user	src	srcname	dst	dstname	dstportname	msg
2015-02-20 15:37:39	fw-milan.corp.local	block	George	10.0.100.10	pc10	37.98.128.65	some.spammer.com	http	Blocked url
2015-02-20 15:37:38	fw-milan.corp.local	block	Poppy	10.0.100.17	pc17	212.73.12.1	www.suspicious.net	http	Blocked url
2015-02-20 15:37:33	fw-lille.corp.local	block	Oliver	10.0.100.1	pc01	22.173.12.1	www.malware.net	http	Blocked url
2015-02-20 15:37:26	fw-milan.corp.local	block	Olivia	10.0.100.12	pc12	37.98.128.65	some.spammer.com	http	Blocked url
2015-02-20 15:37:24	fw-lyon.corp.local	pass	Poppy	10.0.100.17	pc17	10.0.0.5	web.corp.local	http	
2015-02-20 15:37:21	fw-milan.corp.local	block	Mia	10.0.100.20	pc20	52.183.12.13	www.proxy.net	http	Blocked url
2015-02-20 15:37:13	fw-lyon.corp.local	pass	Jacob	10.0.100.4	pc04	10.0.0.3	ssh.corp.local	ssh	
2015-02-20 15:37:11	fw-milan.corp.local	pass	Jessica	10.0.100.14	pc14	216.58.211.73	www.blogspot.com	http	
2015-02-20 15:37:05	fw-milan.corp.local	pass	Thomas	10.0.100.6	pc06	173.194.45.70	www.youtube.com	http	

QUERY / FILTERING

Dashboards display several indicators: bar charts, pie charts, tables or maps. Queries and filters will then allow restricting the data displayed in a dashboard.

Queries

Simple queries

Queries on the database may either be simple or advanced.

Examples:

Searching in logs using the keywords "interactive" or "connection":
interactive connection

To search all terms, simply indicate:
"interactive connection"

Search by a specific field:
alarmid:6

Perform complex searches using operators written in uppercase letters:

ssh AND 10.0.3.30

Combine operators using brackets:

("interactive connection" OR "connection detected") AND 10.0.3.30

i NOTE/REMARK

Operators have to be written in uppercase letters to be taken into account.

Indicate ranges of numerical values in order to search for a port for example:

dstport:[20 TO 23]

This query would also allow displaying only ftp-data [20], ftp[21], ssh [22] and telnet [23] ports.

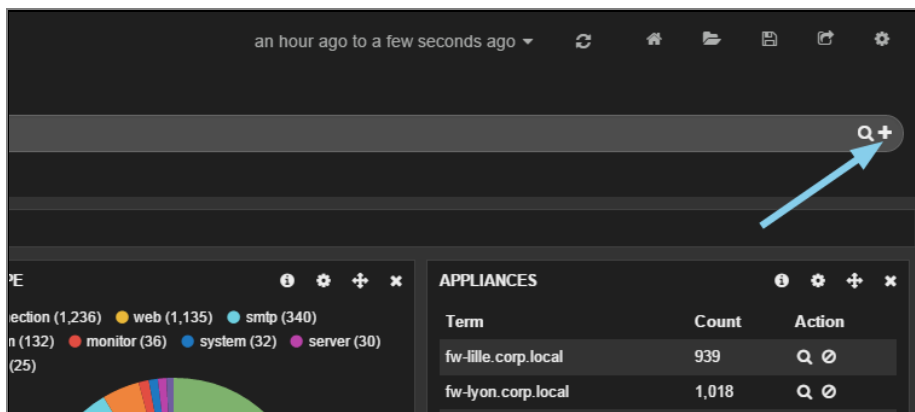
i NOTE/REMARK

The wildcard character ["*"] makes it possible to replace a string of characters in a query.

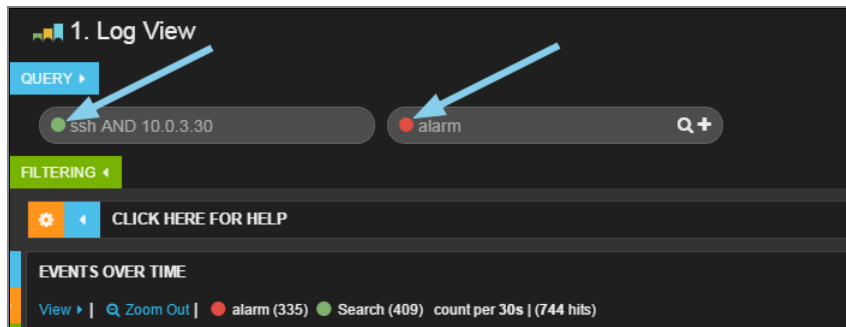
Multiple queries

In certain cases, if you wish to compare the results of two queries, you can link them using the OR operator or separate them into two distinct search fields.

Click on the "+" symbol to the right of the Query field to add a second query:

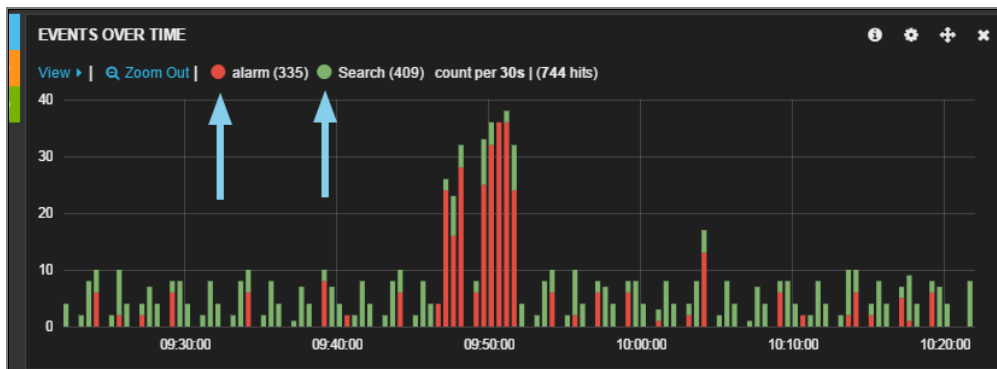



You will then obtain two sections that allow separating the searches:

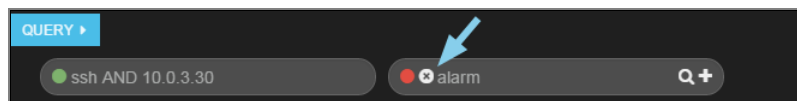


These queries will search logs for all SSH connections with the source or destination IP address 10.0.3.30 (green search) or alarm logs (red search).

The diagrams in the dashboard will be refreshed once the query is sent:

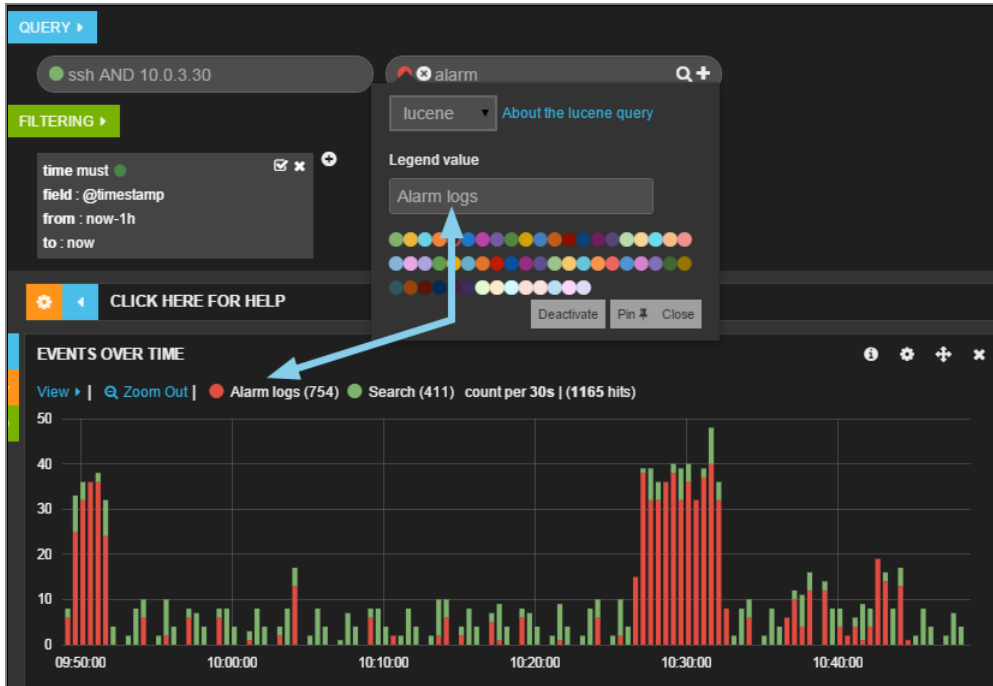


To delete a query, click on  when you scroll your mouse over the relevant query field:



Colors and legends

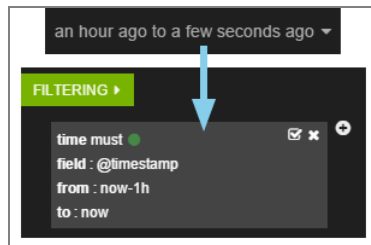
The color of a query is chosen automatically by Log Appliance. However, the server's administrator can customize queries. Simply click on the color button in the query field to display, for example, a drop-down menu that allows you to change the color or assign a new legend to the query.



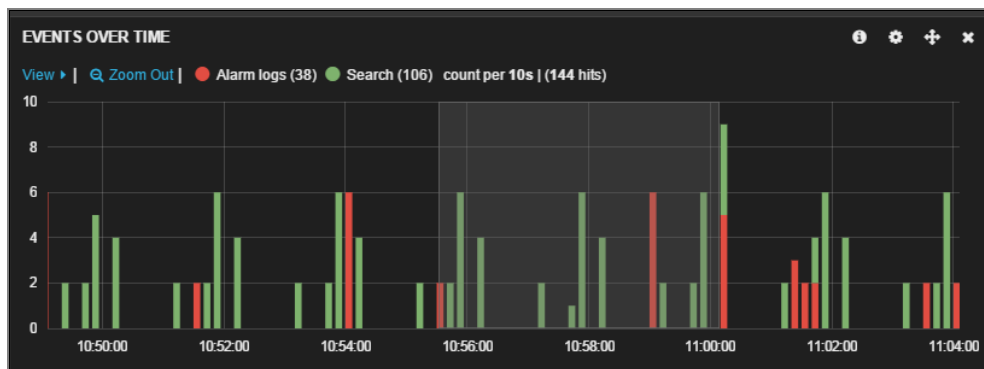
Filters

Time filter

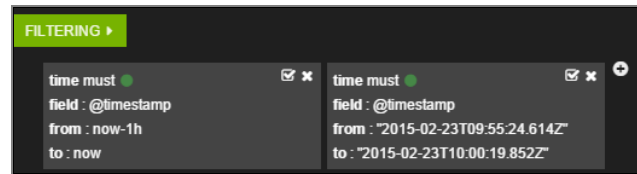
Virtual Log Appliance graphs are interactive and may be filtered with precision in order to search for a value. By default, time filters are applied.



Depending on the time slot chosen, the time filter will be refreshed accordingly. Filtering within a graph is possible by simply selecting the desired period with the mouse:

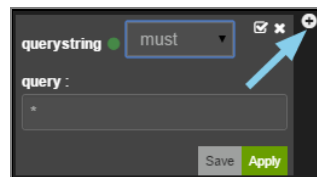


This selection means that a filter will be automatically added to the period selected initially:




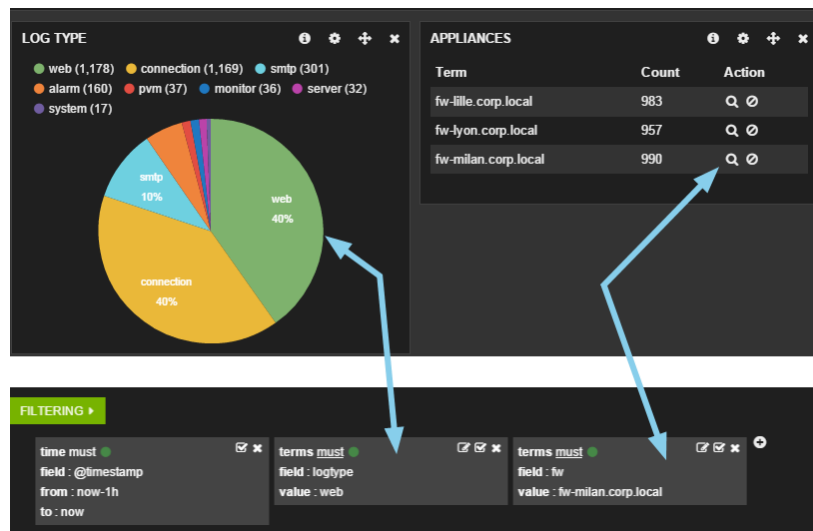
Customized filter

To add a customized filter, simply click on the “+” button and fill in the desired field:



There are two other ways to filter the search within the data.

Click once in the zone around a diagram or on the magnifying glass icon  to create the associated filter in the **Filtering** zone:



This example will return web logs for the firewall named *fw-milan.corp.local* over the selected period.

For each filter created in this way, three buttons located in the header allow, respectively, editing, enabling/disabling or deleting the search.

After a filter is deleted, the data displayed will be automatically refreshed.

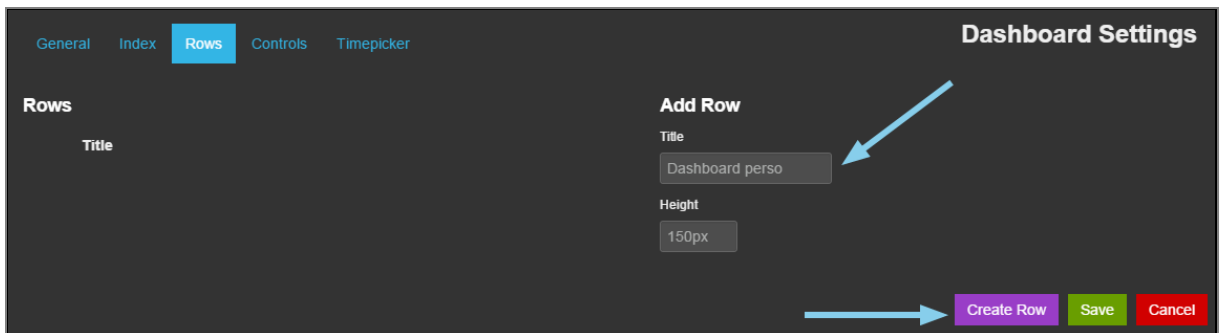
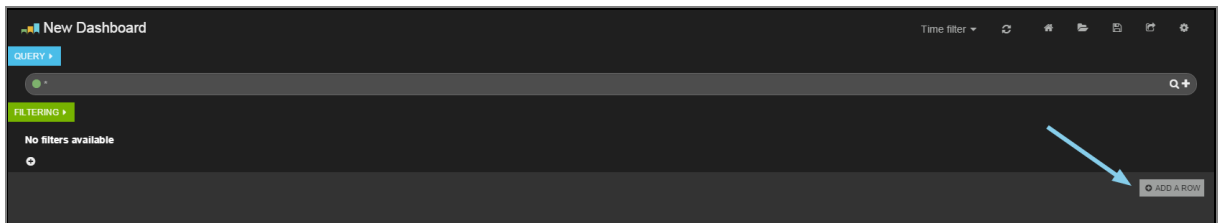
ROWS AND PANELS

Each Virtual Log Appliance dashboard is made up of rows and panels. Tables created by default can be modified but only temporarily (cannot be saved). However, you can arrange customized dashboards according to your preferences.

Rows

Adding a row

Take for example an empty dashboard that we have just created. An "Add a row" button allows adding a row to the dashboard and configuring it:



The new row will appear on the left in the list of rows. Click on Save to confirm its addition.

Managing rows



A new row now appears in your dashboard. Three buttons on the left represent this row and respectively allow:

- Minimizing the row (hide),

i NOTE/REMARK

Queries and filters can also be hidden by clicking on their respective buttons

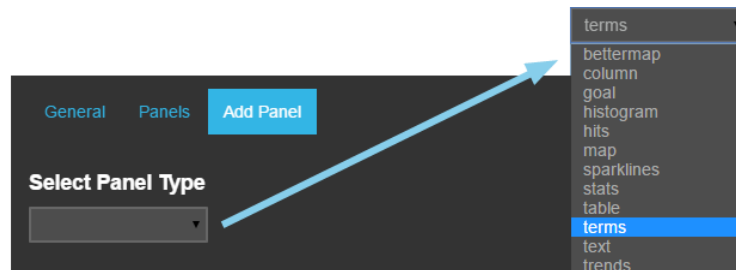
- Configuring the row,
- Adding a panel.

Panels

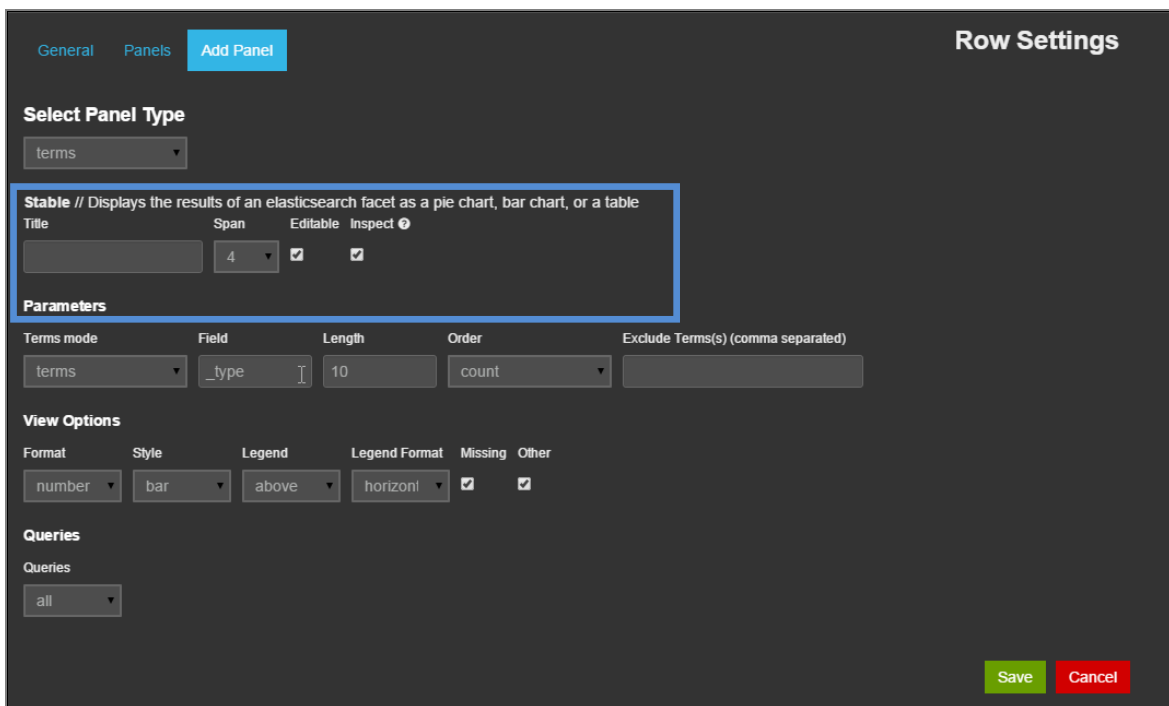
Dashboards are made up of panels which are included in rows and have the main role of displaying the results of queries (simple or multiple) and filters. A panel would include for example a bar chart, pie chart or table summarizing the data searched.

Adding panels

By clicking on the green button (Add Panel), you will be able to select various types of panels depending on what you wish to display:



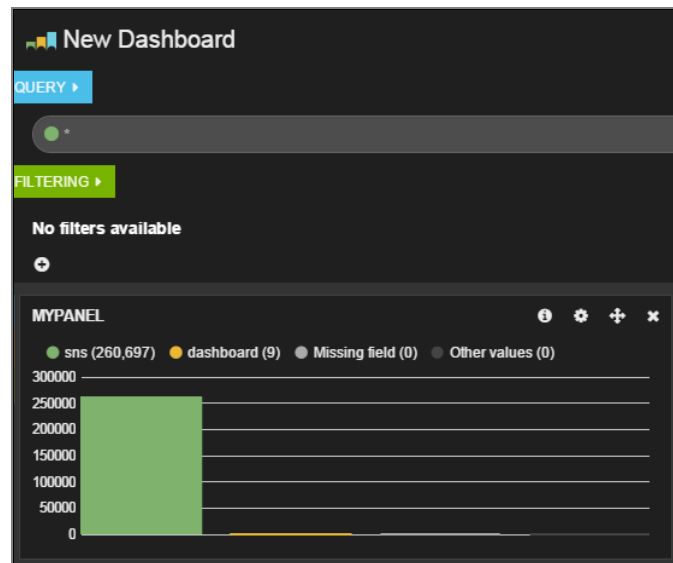
Choose for example a “terms” panel:





The “terms” panel contains many options. Focusing on the general parameters, the first section contains:

- **Title:** name of the panel,
- **Span:** width of the panel. Virtual Log Appliance dashboards are made up of 12 spaces of the same size. Each panel will have a size ranging from 1 to 12,
- **Editable:** if this option is selected, the panel can be modified later,
- **Inspectable:** the user can see the query used by this panel,



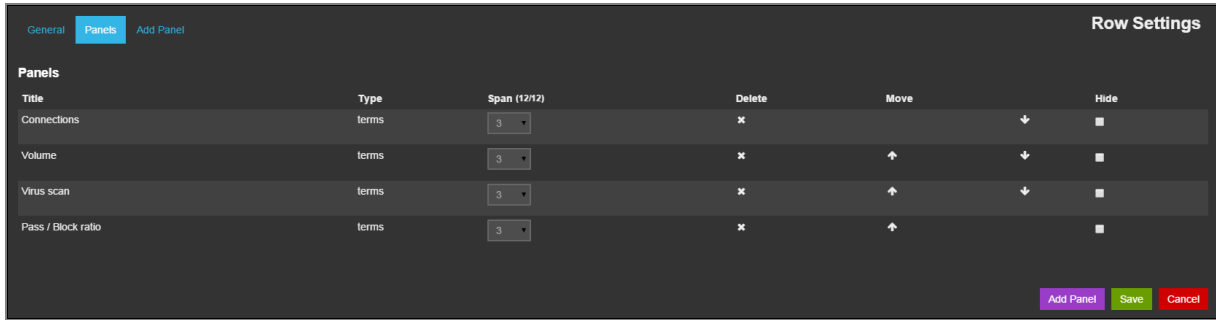
You can now customize the search field by modifying the queries and filters applied to the log database on your Stormshield appliances.

Editing a row


Rows can be renamed, resized and edited. To do so, simply click on the orange button of a row to access its configuration.

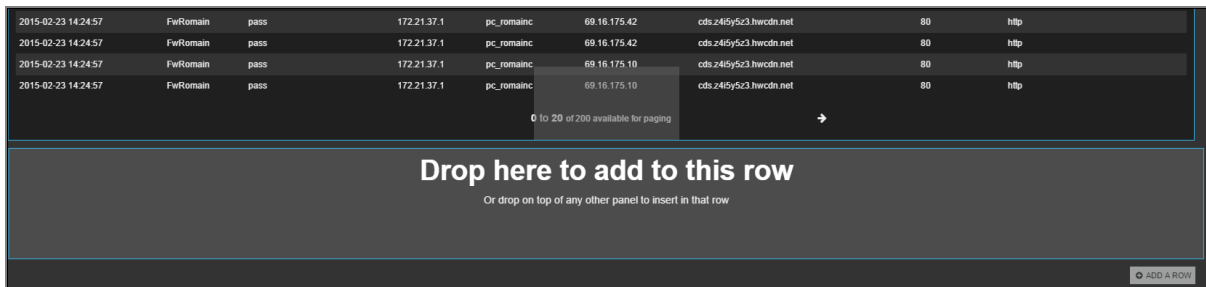
The screenshot shows the 'Row Settings' dialog box. It has three tabs: 'General', 'Panels', and 'Add Panel'. The 'General' tab is active. It contains four fields: 'Title' (with the value 'Traffic'), 'Height' (with the value '150px'), 'Editable' (with a checked checkbox), and 'Collapsible' (with a checked checkbox). At the bottom right, there are two buttons: 'Save' (green) and 'Cancel' (red).

As for the *Panels* tab, it allows modifying the order of panels in the row, modifying their sizes or deleting them.

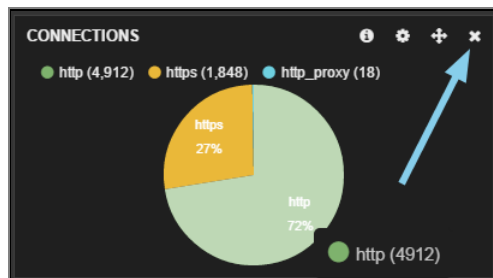


Moving or deleting panels


Panels can be dragged and dropped in the same row or from another row using the move button  located to the top right of the panel.

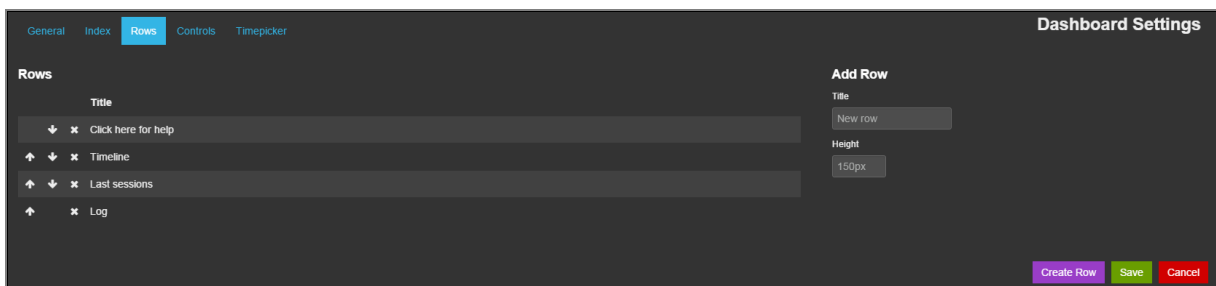


Panels can be deleted by clicking on the cross at the top right of a panel or from the configuration menu of a row, as seen earlier.



Moving or deleting a row

Rows can be moved or deleted in the parameters of the dashboard by clicking on the parameters button  at the top right of the page.






Arrows allow you to change the order of rows according to your preferences.

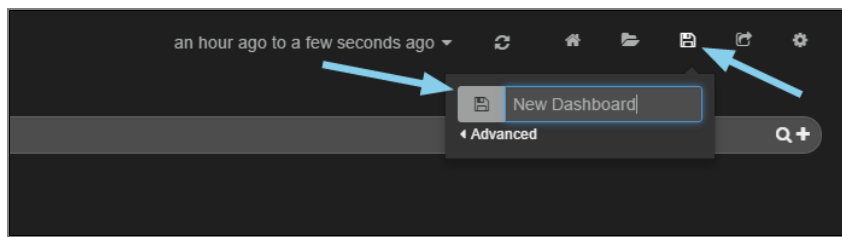
MANAGING DASHBOARDS

After having created your own dashboard, you most certainly would want to share it with other members in your team or set up automatic data refreshment in order to display it on a control screen.


Virtual Log Appliance enables you to save your own dashboards and load them quickly using the button  (“Load”).

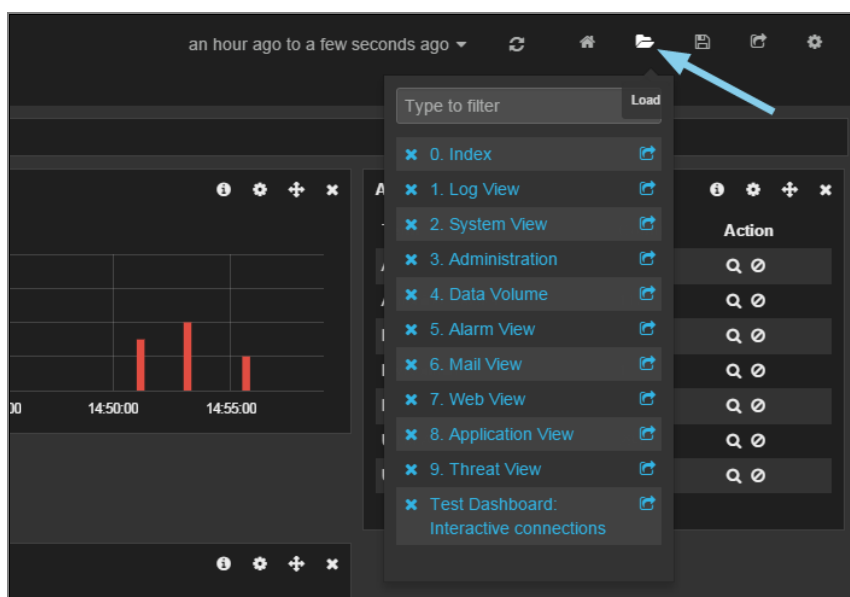
Saving a dashboard

To save your new dashboard, click on the diskette icon at the top right of the screen. Name this view and confirm.




Opening a dashboard

The list of dashboards saved can be accessed through the button  (“Load”) at the top right of the screen. From this menu, you can load, share or delete your dashboards:





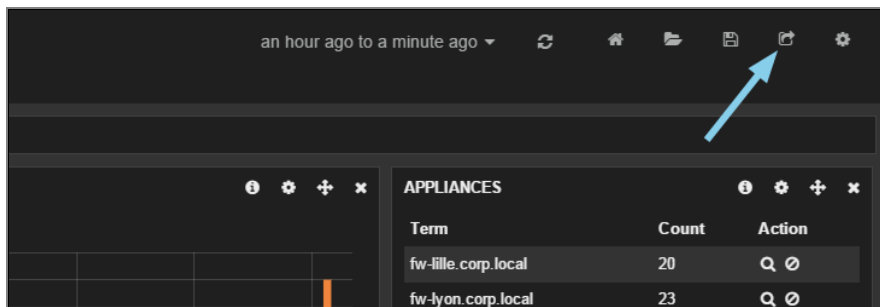
Sharing a dashboard

The button  opens the URL for accessing the selected dashboard in a pop-up.

Example

`https://server_address/#dashboard/elasticsearch/MYTABLE`

You can also generate a temporary link by clicking on the share button in the page's header:



Example

`https://server_address/#dashboard/temp/rb577tScQied4svrAioTMg`

NOTE/REMARK

Temporary links remain valid for 30 days.

Saving a static dashboard

Dashboards can also be saved on the disk in JavaScript Object Notation format (extension “.json”). In this case, the dashboard has to be placed in the folder:
`/opt/kibana/app/dashboards/`

Extracting a dashboard

Do you wish to find out a dashboard's syntax? To do so, simply click on the save button in the dashboard then on **Advanced** in order to extract its contents:



WARNING

Dashboards use the JSON syntax. This is a very strict syntax in which a missing comma or bracket would prevent the table from being loaded.



Automatically refreshing a dashboard

In the time filter selection area, in a dashboard's header, the **Auto-Refresh** option allows automatically refreshing data displayed in the various panels. For example, this allows an administrator to supervise certain counters on machines in his network on his control screen:

