

KIBANA

KIBANA Field filter keywords

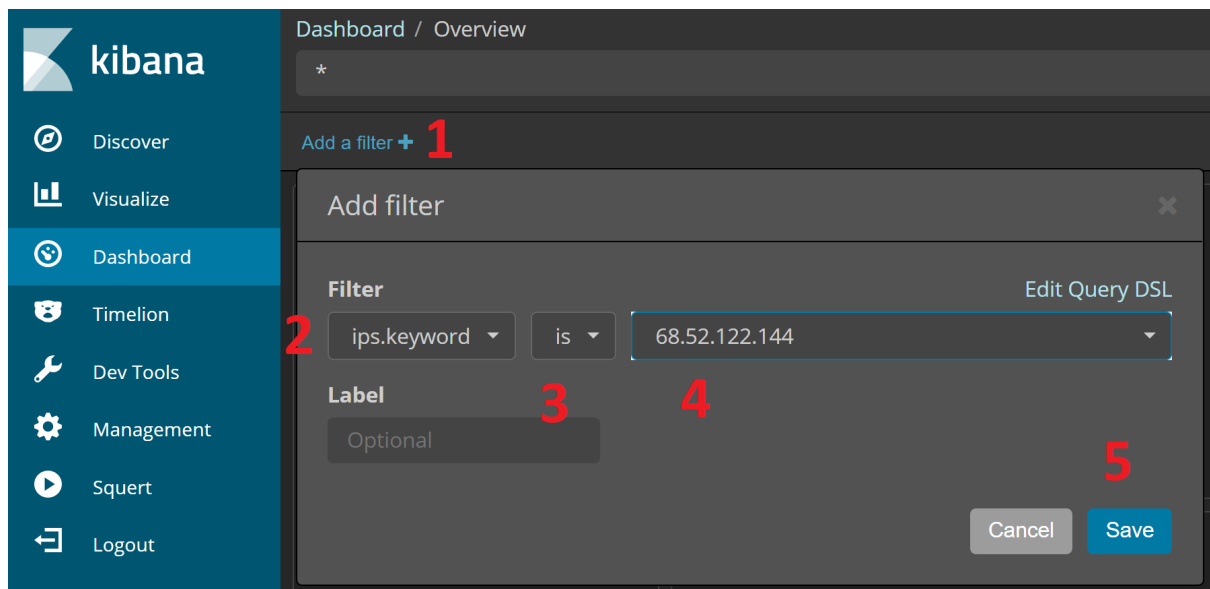
Search by generic IP: **ips.keyword**

Search by source IP: **source_ips.keyword**

Search by destination IP: **destination_ips.keyword**

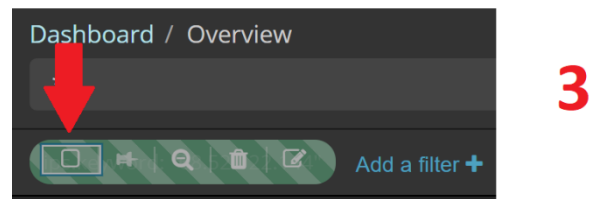
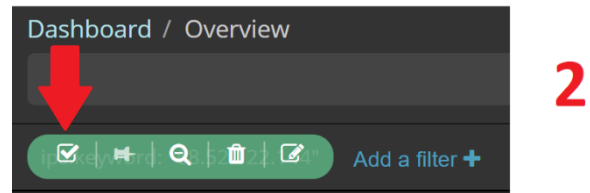
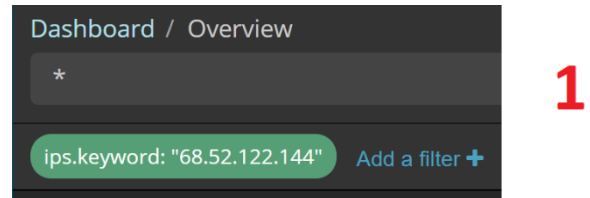
Add a filter

1. On top left, click on “Add a filter +”. A menu will open;
2. In the textbox “Fields...” write the kind of resource you’re looking for (examples provided below)
3. In “Operators...” write **is** or **is not**;
4. In “Values” the IP or port you’re looking for;
5. Click on save.



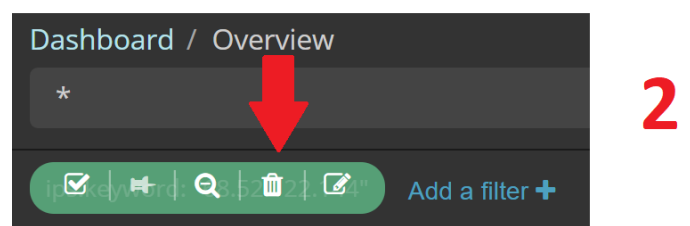
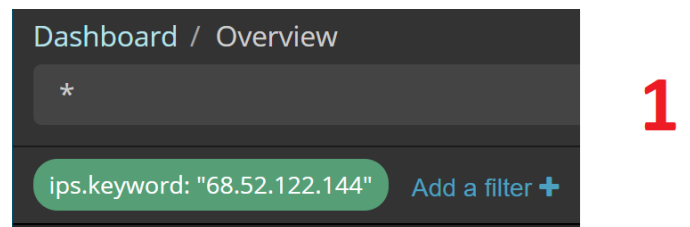
Temporarily disable filter

1. Move the mouse over the filter you want to disable;
2. Click on the checkbox icon (first icon to left);
3. Click it again to re-enable the filter.



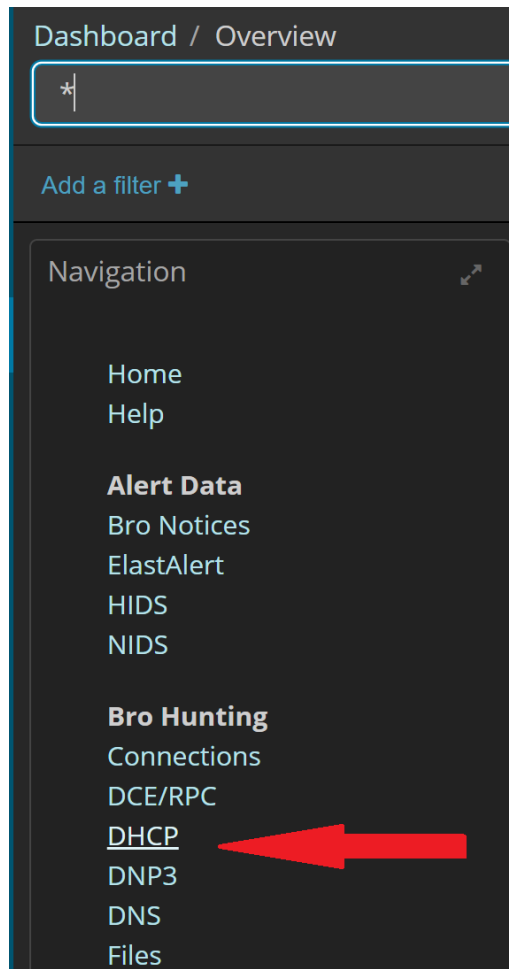
Delete filter

1. Move the mouse over the filter you want to delete;
2. Click on the trash bin icon (second from the right).

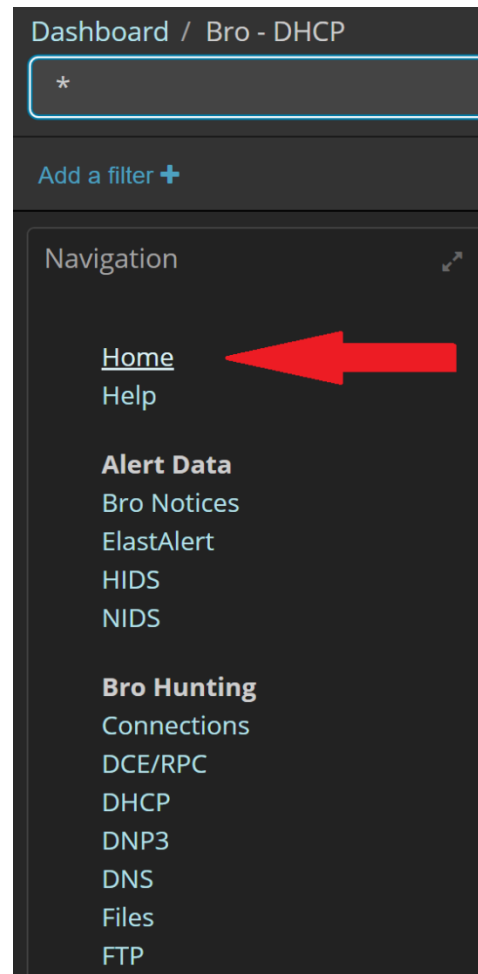


Filter by service/protocol

1. On the left, click on the required service/protocol;
2. To disable this filter, click on “*Home*” on top of the same list.



1



2

SQUERT

Filter by alert priority

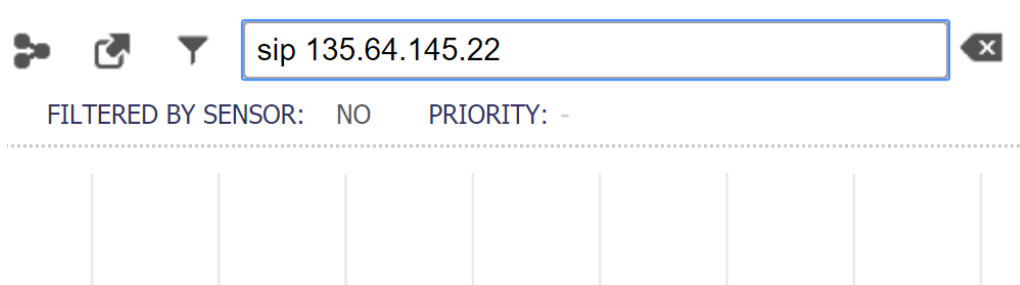
1. On top right, under “Filter”, there can be three bars. Red for high, orange for medium, yellow for low priority;
2. Click on a priority to filter the alerts accordingly;
3. Clicking again on the same priority, will disable the filter.



SQUERT Field filter keywords

Search by generic IP: **ip**
Search by source IP: **sip**
Search by destination IP: **dip**

Set a filter



1. On top right, write in the “Filter” textbox filter followed by the IP address.
2. Press enter.

Unwrap alerts and explore

1. On the list of alerts, click one of interest clicking on the number of events;
2. From here, a list will expand with the events grouped by source-destination. Click on the number of alerts to expand;
3. Now you have the single events involving those two parts. Click on RT to expand;
4. From here, you get the details about the single event, such as content and signature.

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE
3000	147	645		16:17:15	ET SCAN Potential SSH Scan

1

3002	147	645		16:17:15	ET SCAN Potential SSH Scan
<p>alert tcp \$EXTERNAL_NET any -> \$HOME_NET 22 (msg:"ET SCAN Potential SSH Scan"; flags:S,12; threshold: type both, track by_src, count 5, seconds 120; 219; classtype:attempted-recon; sid:2001219; rev:19; metadata:created_at 2010_07_30, updated_at 2010_07_30;)</p> <p>file: downloaded.rules:11545</p> <p><input checked="" type="checkbox"/> CATEGORIZE 3002 EVENT(S) CREATE FILTER: src dst both</p>					
QUEUE	ACTIVITY	LAST EVENT	SOURCE		
1		2019-11-27 16:18:17	<input type="checkbox"/> 51.83.74.203		
478		2019-11-27 16:17:57	<input type="checkbox"/> 131.155.21.156		

2

479

3

RT

2019-11-27 15:29:00

[2.15390294](#)

104.244.79.146

34104

131.155.71.154

22

ET SCAN LibSSH Based Frequent SSH C

COMMENTS

None.

TAGS

None.

PAYLOAD

IP	VER	IHL	TOS	LENGTH	ID	FLAGS	OFFSET					
	4	5	0	60	0	0	0					
TCP	R1	R0	URG	ACK	PSH	RST	SYN	FIN	SEQ#	ACK#	OFFSET	RES
	0	0	0	0	0	0	0	0	0	0	5	0
DATA	HEX	ASCII										
	53 53 48 2D 32 2E 30 2D 6C 69 62 73 73 68 2D 30 2E 31 0D 0A	SSH-2.0-libssh-0.1..										
ASCII	SSH-2.0-libssh-0.1..											

4