

SIEM Software

CS457 Lab - Andy, Cary, Chuck, Juno

Prerequisites

- Ubuntu Linux computer or VM
 - 4 CPU cores / 8 GB RAM or more recommended
 - Image provided
- The following packages:
 - `docker.io`
 - `docker-compose-v2`
 - `git`
- We provide a ready-to-run Ubuntu VM image if you need it.
 - No packages installed on it yet

Installing Wazuh

- Download the lab repository
- `cd` to the `software/wazuh-server` directory
- Run `start.sh`
- Go to <https://localhost> in your browser
 - Accept the security popup if you get one
- Log into the admin account
 - Username: `admin`
 - Password: `SecretPassword`
- Don't do anything else yet - we have just a bit more setup to do.



Installing the Wazuh agent

- `cd` to the `software/wazuh-agent` directory
 - Run `install.sh`
 - This sets up the Wazuh repo and installs the Wazuh agent package.
 - Run `start.sh` to enable and start the Wazuh agent.
-
- The other scripts let you stop and uninstall the Wazuh agent after the lab.

Tour: Login

- Go to <https://localhost> in your browser
 - Accept the security popup if you get one
- Log into the admin account
 - Username: `admin`
 - Password: `SecretPassword`

A login form with a white background and a thin grey border. It contains two input fields: the first for the username "admin" with a user icon, and the second for the password "SecretPassword" with a lock icon. Below the fields is a blue "Log in" button.

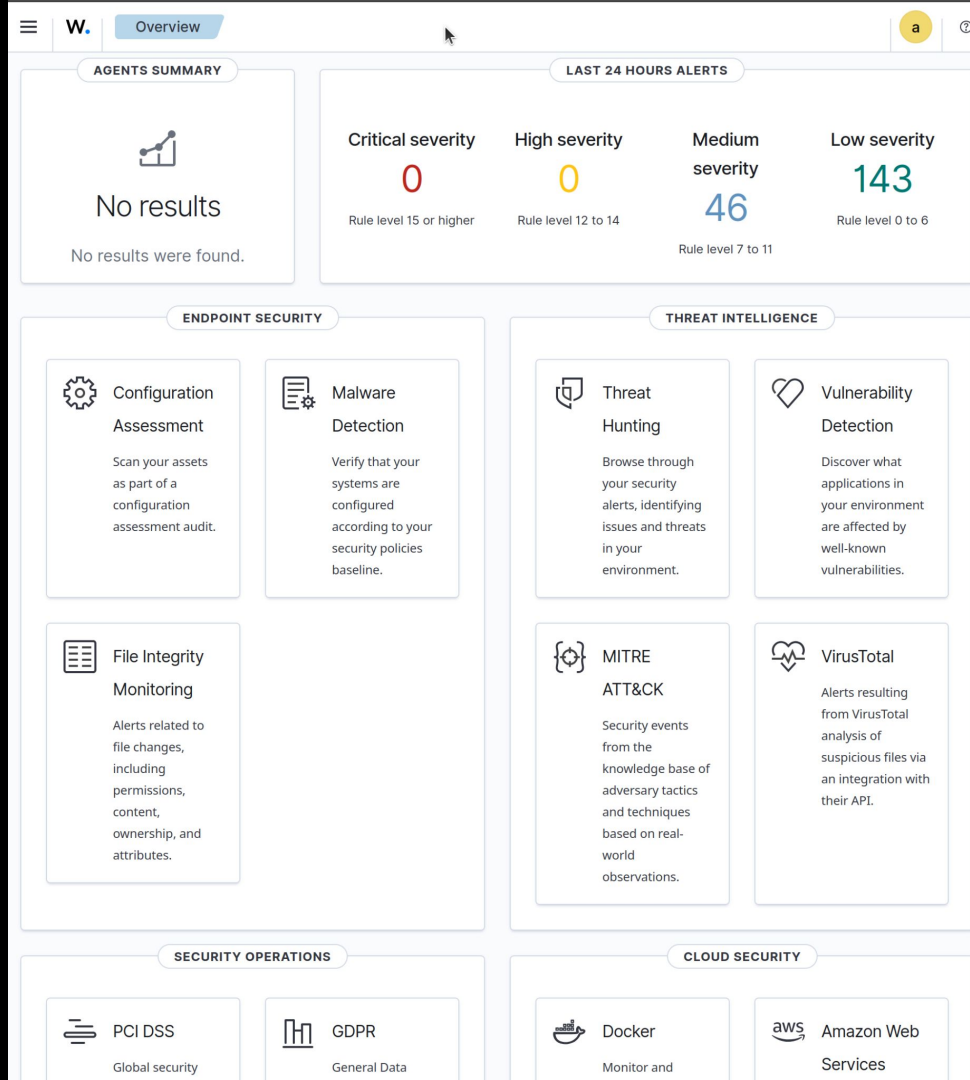
	admin
	SecretPassword
<button>Log in</button>	

Tour: Dashboard

The first page you will see after logging in is Wazuh's dashboard.

We won't spend much time here. Most of the useful stuff is in the left sidebar.

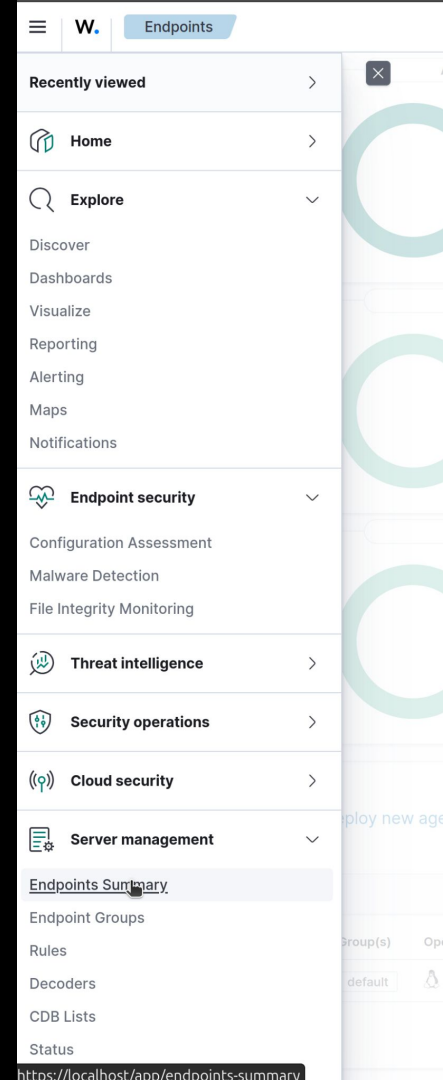
(open with the ☰ icon in the top left)



Tour: Sidebar

Most of what we'll focus on in the lab is in the “Explore” section. This section lets you manually sift through data, as well as create charts and alerts.

Let's go to “**Endpoints Summary**” in the “Server management” section to make sure the Wazuh agent you installed earlier is connected.



Tour: Endpoints Summary

If your agent is connected, you should see something like this.

If this is not the case, restart the Wazuh server first (stop.sh, then start.sh), then restart the Wazuh agent (stop.sh, then start.sh).

Agents (1)

[Deploy new agent](#)

[Refresh](#)

[Export formatted](#)

[More](#)

☐ Show only outdated

Search

WQL

<input type="checkbox"/>	ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
<input type="checkbox"/>	001	juno-laptop	127.0.0.1	default	Ubuntu 24.04.1 LTS	node01	v4.9.2	● i	👁 ⋮

Rows per page: 10

[<](#) [1](#) [>](#)

Tour: Explore Tab

We will focus on the following in this lab:

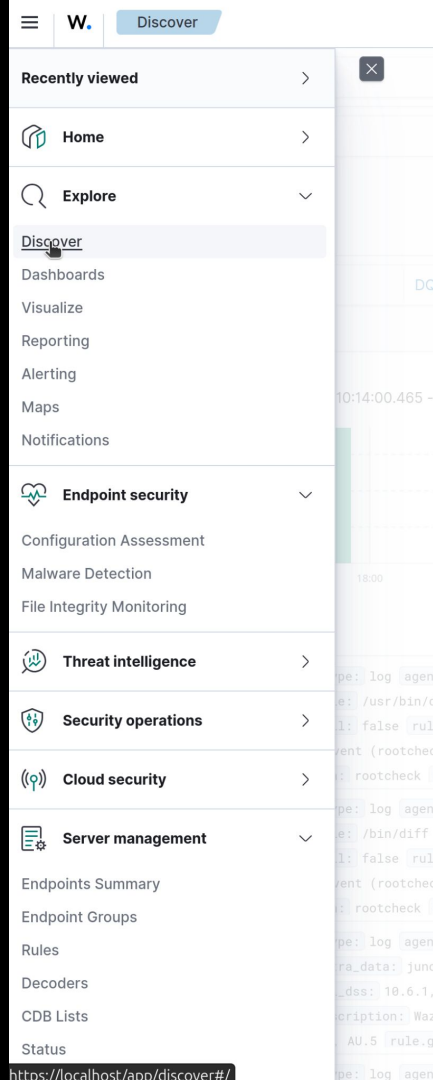
Discover: Manually filter and view events.

Dashboards: Assemble tables and charts into pages.

Visualize: Create tables and charts for Dashboards.

Alerting: Fire alerts when conditions are met.

Let's go to "Discover" first.



Tour: Generate some events

Before we check out the Discover page, let's generate a couple authentication events.

Run `sudo su` and type your password to switch to the root user.

Do this again, but with an incorrect password.

```
juno@juno-laptop:~$ sudo su
[sudo] password for juno:
root@juno-laptop:/home/juno#
```

Tour: Discover

Discover lets you see the actual stream of events the software is working with.

Click “+ **Add filter**” to start finding the events we just created.

wazuh-alerts-*

Search field names

Selected fields ▾

_source

Available fields ▾

Search

DQL

Calendar icon

Last 24 hours

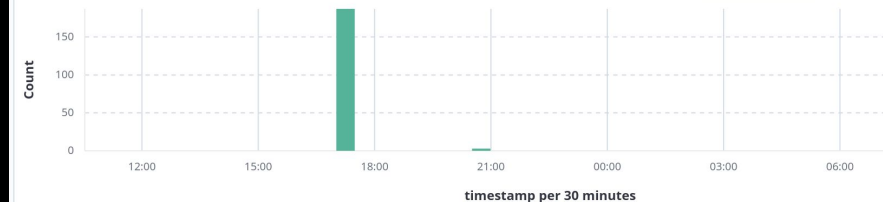
Show dates

+ Add filter

218 hits

Nov 29, 2024 @ 10:31:35.429 - Nov 30, 2024 @ 10:31:35.429 per

Auto



Time ↓

_source

```
> Nov 30, 2024 @ 10:20 (+) (-) {
  precoder.hostname: juno-laptop precoder.program_name: sudo precoder.ti
5:20:52 input.type: log agent.ip: 127.0.0.1 agent.name: juno-laptop agent.
manager.name: wazuh.manager data.dstuser: root rule.firedtimes: 8 rule.mai
rule.level: 3 rule.pci_dss: 10.2.5 rule.hipaa: 164.312.b rule.tsc: CC6.8,
rule.description: PAM: Login session closed. rule.groups: pam, syslog rule.

> Nov 30, 2024 @ 10:20 (+) (-) {
  precoder.hostname: juno-laptop precoder.program_name: su precoder.tim
5:20:52 input.type: log agent.ip: 127.0.0.1 agent.name: juno-laptop agent.
manager.name: wazuh.manager data.dstuser: root rule.firedtimes: 7 rule.mai
rule.level: 3 rule.pci_dss: 10.2.5 rule.hipaa: 164.312.b rule.tsc: CC6.8,
rule.description: PAM: Login session closed. rule.groups: pam, syslog rule.

> Nov 30, 2024 @ 10:20 (+) (-) {
  precoder.hostname: juno-laptop precoder.program_name: su precoder.tim
5:20:52 input.type: log agent.ip: 127.0.0.1 agent.name: juno-laptop agent.
manager.name: wazuh.manager data.srcuser: juno data.uid: 0 data.dstuser: r
rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5 rule.hipaa: 164.312.b
CC7.2, CC7.3 rule.description: PAM: Login session opened. rule.groups: pam,

> Nov 30, 2024 @ 10:20 (+) (-) {
  precoder.hostname: juno-laptop precoder.program_name: sudo precoder.ti
```

Tour: Filters

This filter (`rule.groups is authentication_success`) will show only events that involve someone successfully logging in.

Click “**Save**” to apply the filter.

The screenshot shows a user interface for editing a filter. At the top, there is a search bar with a dropdown arrow, a 'DQL' button, and a date range selector set to 'Last 24 hours'. Below this is a '+ Add filter' button. The main part of the interface is a modal dialog titled 'EDIT FILTER' with a link 'Edit as Query DSL' in the top right corner. Inside the dialog, there are two columns: 'Field' and 'Operator'. The 'Field' column has a dropdown menu with 'rule.groups' selected. The 'Operator' column has a dropdown menu with 'is' selected. Below these columns is a 'Value' section with a dropdown menu showing 'authentication_success'. At the bottom of the dialog, there is a toggle switch labeled 'Create custom label?' which is currently turned off. In the bottom right corner of the dialog, there are two buttons: 'Cancel' and 'Save'.

Count

Search

DQL

Last 24 hours

+ Add filter

EDIT FILTER

Edit as Query DSL

Field

rule.groups

Operator

is

Value

authentication_success

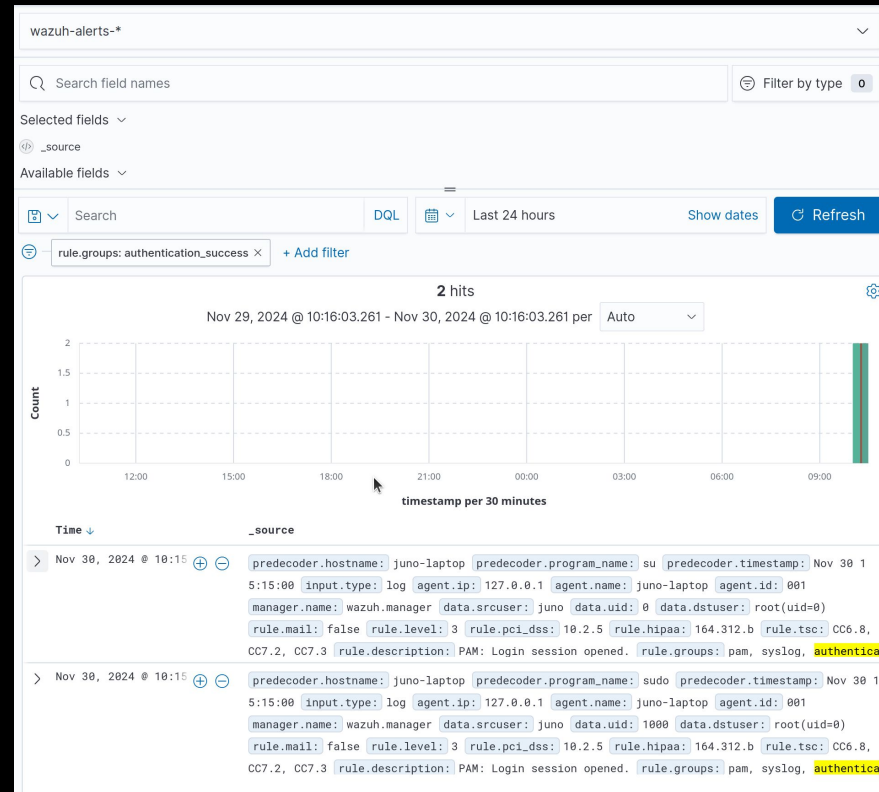
☐ Create custom label?

Cancel


Save

Tour: Using Discover

With the new filter applied, you should see an event that was generated when you logged in as root.






Tour: Viewing Events

Clicking on the  button on the event will let you see all its fields. You can add a filter for any field in an event to further trim down results.




wazuh-alerts-*


Search field names Filter by type 0

Selected fields   _source

Available fields 

timestamp per 30 minutes

Time  Nov 30, 2024 @ 18:15  

 _source

predecoder.hostname: juno-laptop predecoder.program_name: su predecoder.timestamp: Nov 30 15:15:00 input.type: log agent.ip: 127.0.0.1 agent.name: juno-laptop agent.id: 001 manager.name: wazuh.manager data.srcuser: juno data.uid: 0 data.dstuser: root(uid=0) rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5 rule.hipaa: 164.312.b rule.tsc: CC6.8, CC7.2, CC7.3 rule.description: PAM: Login session opened. rule.groups: pam, syslog, authentication



Expanded document View surrounding documents  View single document 

Table JSON

f _index	wazuh-alerts-4.x-2024.11.30
f agent.id	001
f agent.ip	127.0.0.1
f agent.name	juno-laptop
f data.dstuser	root(uid=0)
f data.srcuser	juno
f data.uid	0
f decoder.name	pam
f decoder.parent	pam
f full_log	Nov 30 15:15:00 juno-laptop su[28027]: pam_unix(su:session): session opened for user root(uid=0) by juno(uid=0)
f id	1732979701.3978
f input.type	log
f location	journalid
f manager.name	wazuh.manager
f predecoder.hostname	juno-laptop

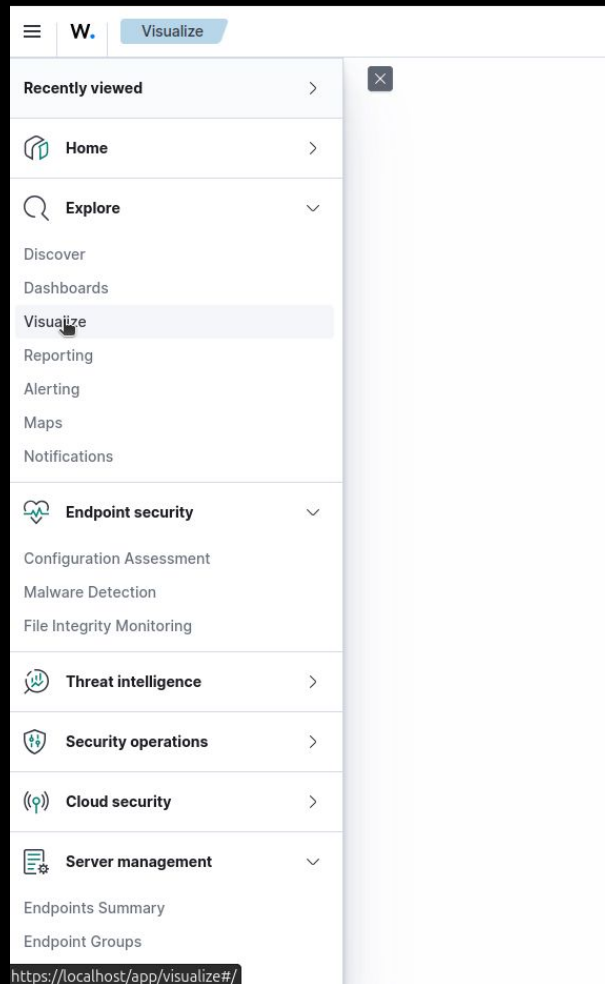
**Groups of filters
(queries) are the basis
for most other features
of the software.**

Tour:

Creating a Chart

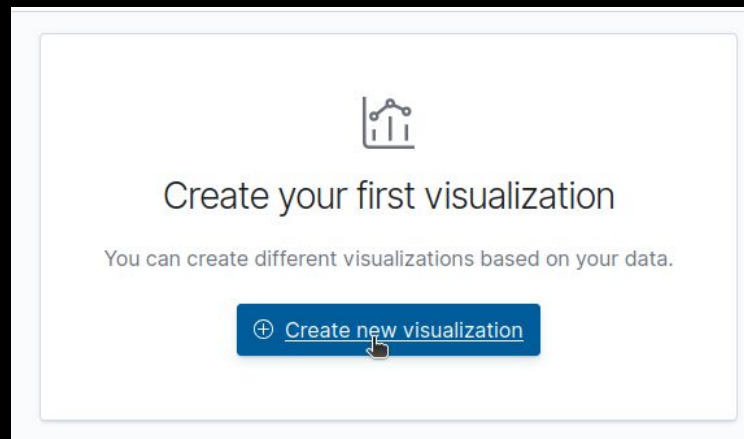
Tour: Creating a Chart (1/12)

In the sidebar, click “Visualize”.



Tour: Creating a Chart (2/12)

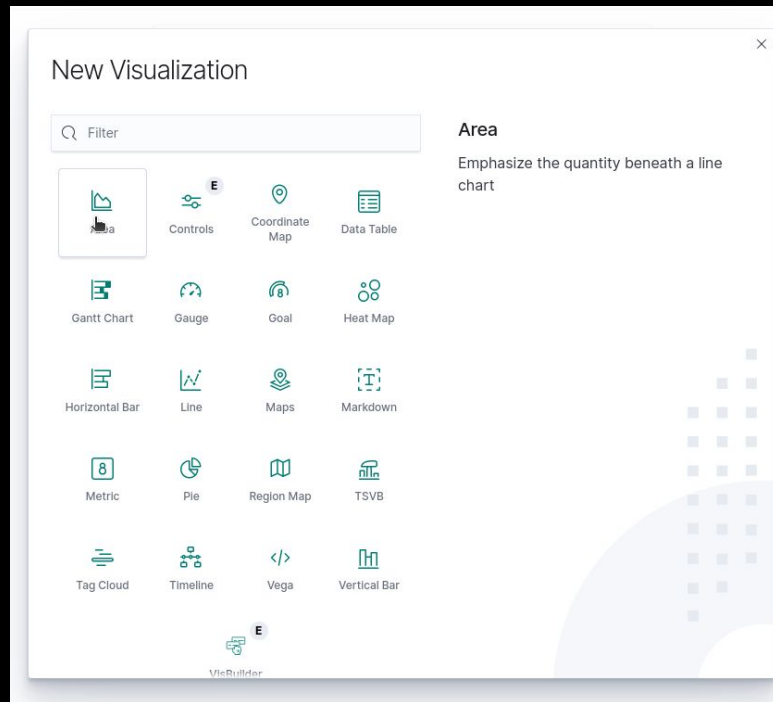
Click “Create new visualization”.



Tour: Creating a Chart (3/12)

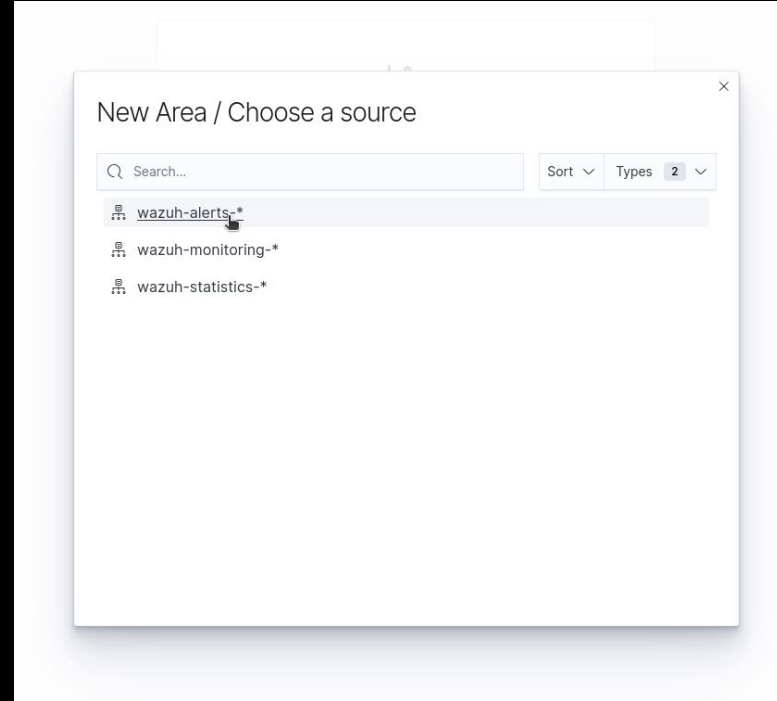
Click “Area”.

If you’d like to create a different kind of chart or table, you can select it here.



Tour: Creating a Chart (4/12)

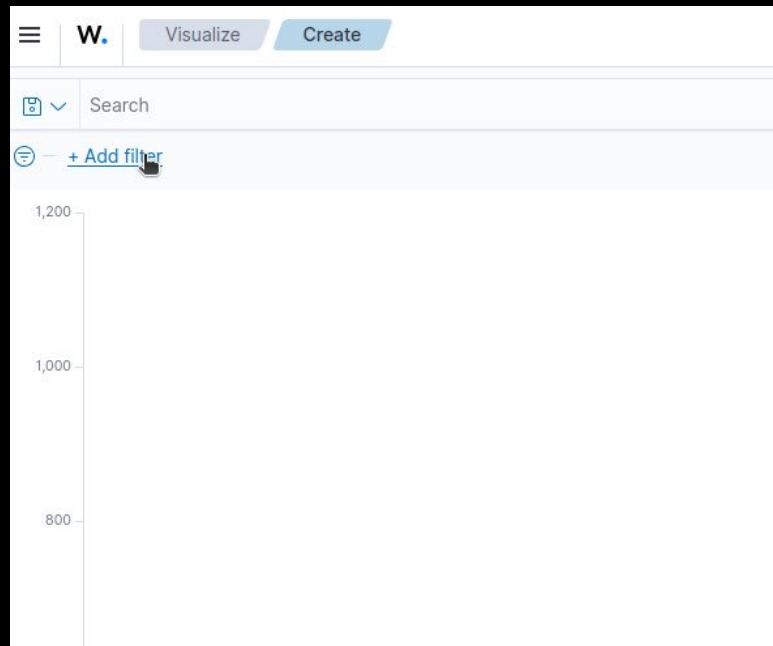
Click “wazuh-alerts-*”.



Tour: Creating a Chart (5/12)

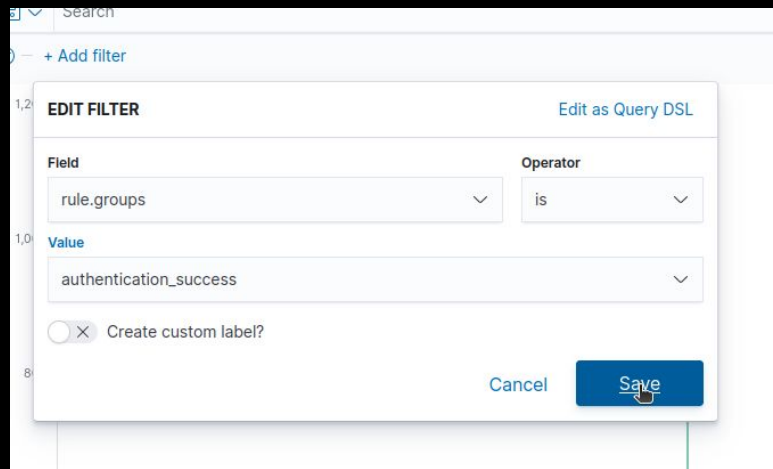
Now you're ready to create the chart.

Click “Add filter” to start.



Tour: Creating a Chart (6/12)

Fill in the filter with the same group we did before (authentication_success) and click “Save”.



The screenshot shows a web interface with a search bar at the top. Below it, there's a '+ Add filter' button. A modal dialog titled 'EDIT FILTER' is open, featuring a link 'Edit as Query DSL' in the top right. The dialog has two columns: 'Field' and 'Operator'. The 'Field' column contains a dropdown menu with 'rule.groups' selected. The 'Operator' column contains a dropdown menu with 'is' selected. Below these, there's a 'Value' section with a dropdown menu showing 'authentication_success'. At the bottom left of the dialog, there's a radio button labeled 'Create custom label?'. At the bottom right, there are two buttons: 'Cancel' and 'Save'.

Search

+ Add filter

EDIT FILTER [Edit as Query DSL](#)

Field	Operator
rule.groups	is

Value

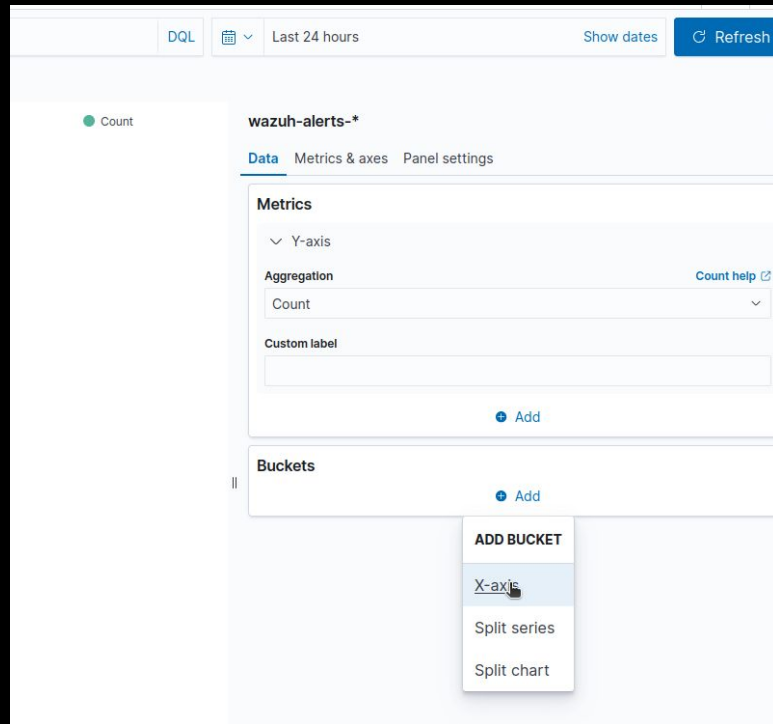
authentication_success

☐ Create custom label?

Cancel Save

Tour: Creating a Chart (7/12)

On the right panel, click “+ Add” under Buckets.
Click “X-axis” in the dropdown.



Tour: Creating a Chart (8/12)

For the aggregation, select “Date Histogram”.

The screenshot shows the configuration interface for a Wazuh alert panel titled "wazuh-alerts-*". It features two tabs: "Data" (active) and "Panel settings".

Metrics Section:

- Y-axis: A dropdown menu currently showing "Count". A "Count help" link is visible to the right.
- Custom label: An empty text input field.
- Bottom: An "Add" button with a plus icon.

Buckets Section:

- X-axis: A dropdown menu currently showing "Date Histogram". A "Date Histogram help" link is visible to the right.
- Below the dropdown is a list of aggregation options: "Date Histogram" (highlighted with a blue bar and a checkmark), "Date Range", "Filters", "Histogram", and "IPv4 Range".

Tour: Creating a Chart (9/12)

For the minimum interval, select “Minute”.

The screenshot shows a configuration panel for a chart. The 'Buckets' section is expanded, showing the following settings:

- X-axis:** Visible (eye icon), Hidden (X icon).
- Aggregation:** Date Histogram (with a help link).
- Field:** timestamp.
- Minimum Interval:** Minute (with a dropdown arrow).
- Currently scaled to 10 minutes** (with a help icon).
- Select an option or create a custom value.** Examples: 30s, 20m, 24h, 2d, 1w, 1M.
- Drop partial buckets:** Unchecked.
- Custom label:** Empty text field.
- Advanced:** Collapsible section.

There are '+ Add' buttons at the top and bottom of the configuration area.

Tour: Creating a Chart (10/12)

Click “Update” to see the chart.

+ Add

Buckets

▼ X-axis

Date Histogram help

Aggregation

Date Histogram

▼

Field

timestamp

▼

Minimum interval

Minute

Currently scaled to 10 minutes

Select an option or create a custom value. Examples: 30s, 20m, 24h, 2d, 1w, 1M

☐ Drop partial buckets

Custom label

> Advanced

+ Add

×

Discard

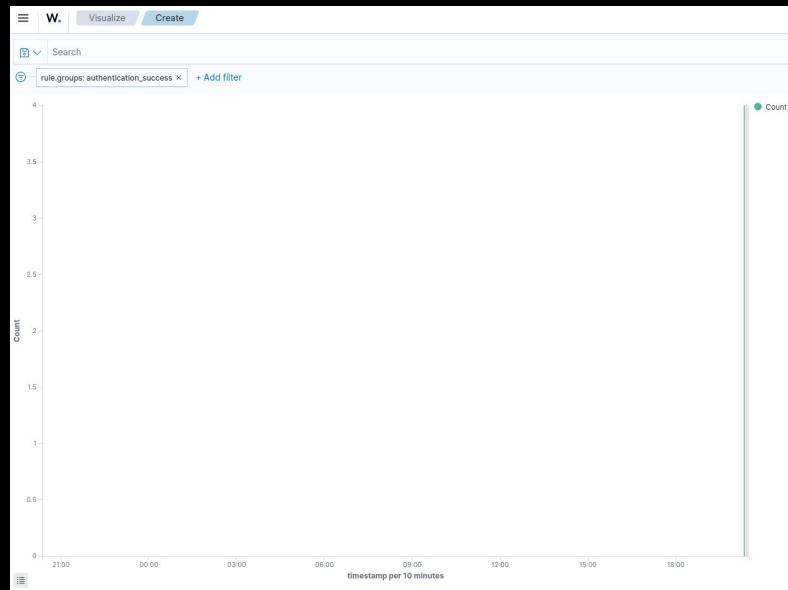
▶

Update

Tour: Creating a Chart (11/12)

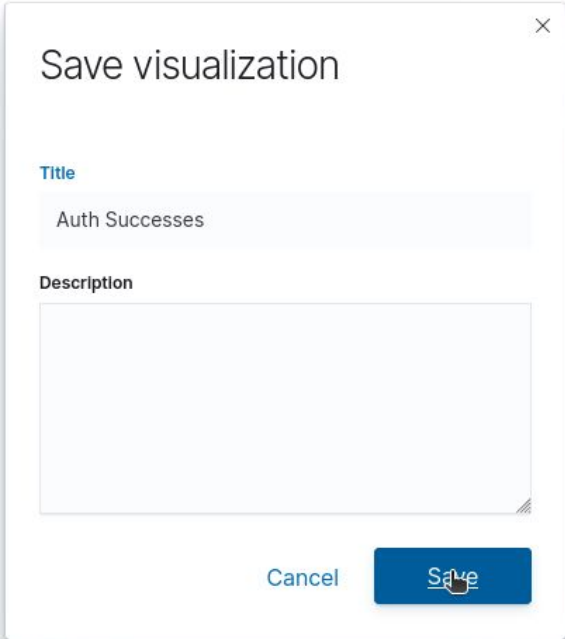
You should see a chart showing successful login attempts.

In this example, I *sudoed* right before clicking “Update”.



Tour: Creating a Chart (12/12)

Name the visualization and click “Save”.



A dialog box titled "Save visualization" with a close button (X) in the top right corner. It contains two input fields: "Title" and "Description". The "Title" field is currently filled with the text "Auth Successes". The "Description" field is empty. At the bottom right, there are two buttons: "Cancel" and "Save". A mouse cursor is hovering over the "Save" button.

Save visualization

Title

Auth Successes

Description

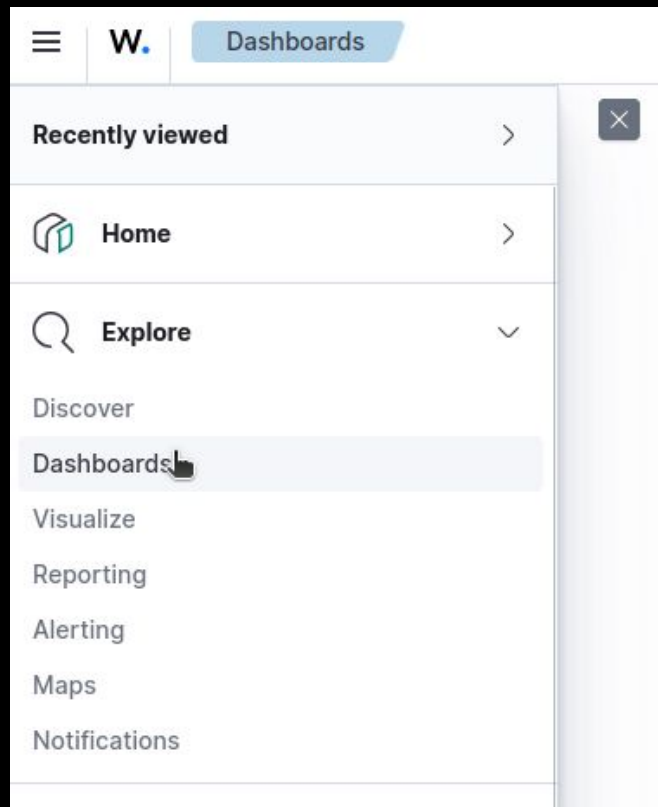
Cancel Save

Tour:

Creating a Dashboard

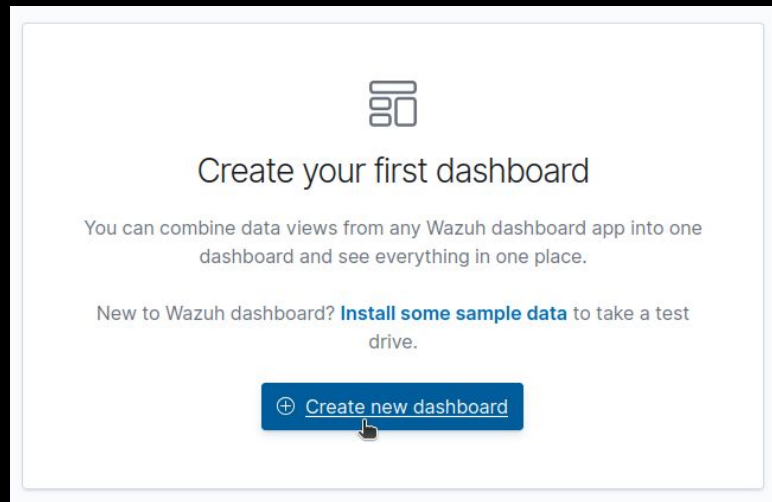
Tour: Creating a Dashboard (1/6)

Click “Dashboards” in the sidebar.



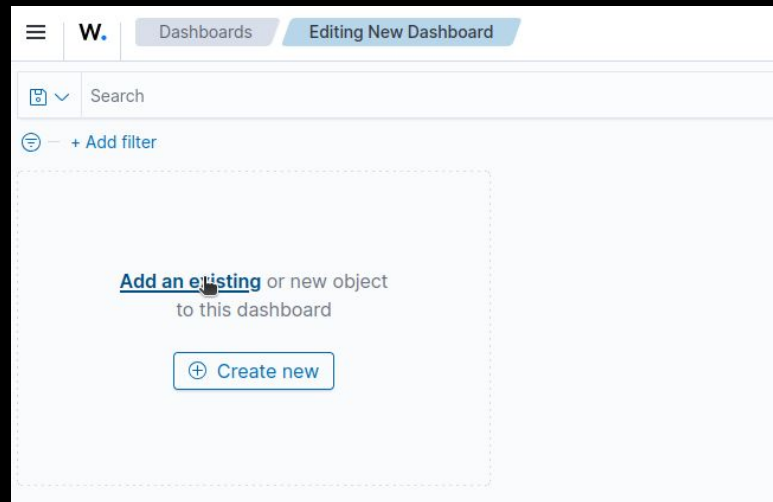
Tour: Creating a Dashboard (2/6)

Click “Create new dashboard”.



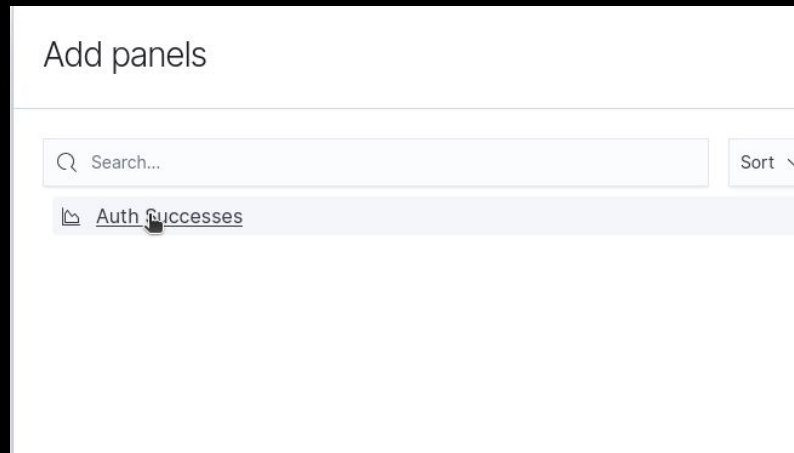
Tour: Creating a Dashboard (3/6)

Click “Add an existing [...] object to this dashboard”.



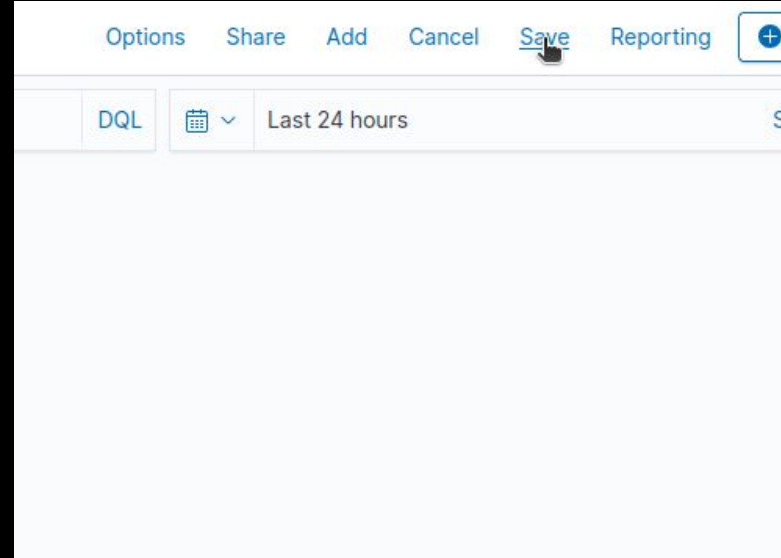
Tour: Creating a Dashboard (4/6)

Click on the chart we created earlier.



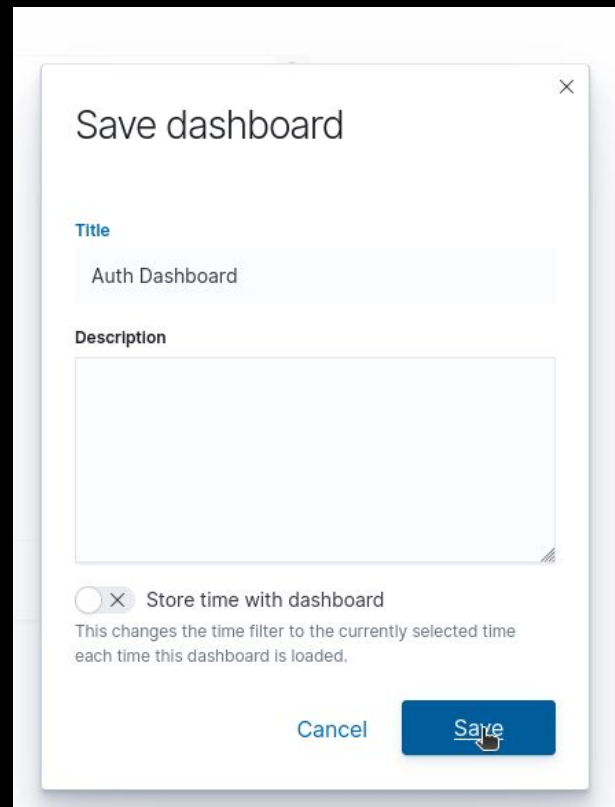
Tour: Creating a Dashboard (5/6)

Click “Save”.



Tour: Creating a Dashboard (6/6)

Fill in a name and click “Save”.



The screenshot shows a 'Save dashboard' dialog box with a close button (X) in the top right corner. The dialog contains a 'Title' label followed by a text input field containing 'Auth Dashboard'. Below this is a 'Description' label followed by a large, empty text area. At the bottom, there is a toggle switch labeled 'Store time with dashboard' which is currently turned off. Below the toggle is a descriptive text: 'This changes the time filter to the currently selected time each time this dashboard is loaded.' At the bottom right, there are two buttons: 'Cancel' and 'Save'. A mouse cursor is pointing at the 'Save' button.

Save dashboard

Title

Auth Dashboard

Description

☐ Store time with dashboard

This changes the time filter to the currently selected time each time this dashboard is loaded.

Cancel Save

Tour:

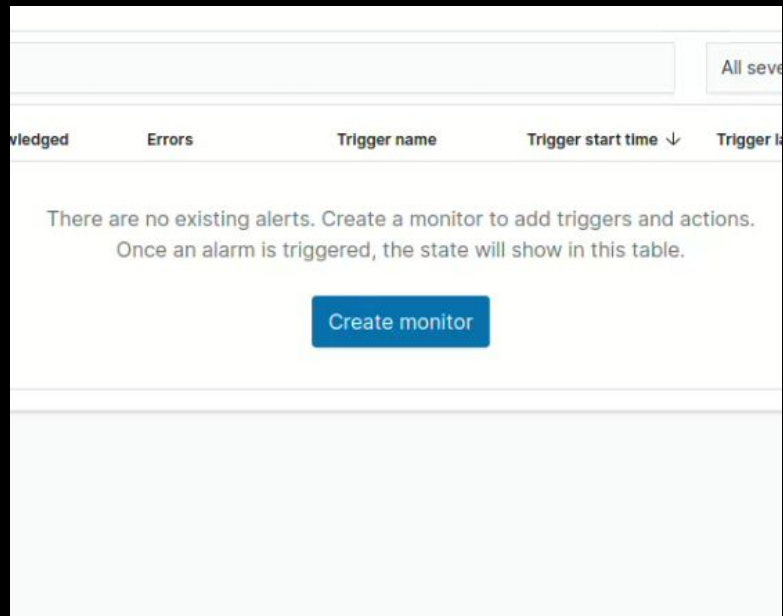
Creating an Alert

Tour: Creating an Alert (1/9)

Navigate to “Alerting” in the sidebar.

Tour: Creating an Alert (2/9)

Click “Create Monitor”.



Tour: Creating an Alert (3/9)

Fill in a name for the monitor.

The screenshot shows the 'Create monitor' form in a web application. The top navigation bar includes a hamburger menu, a 'W.' logo, and three tabs: 'Alerting', 'Monitors', and 'Create monitor'. The main heading is 'Create monitor'. Below it is a section titled 'Monitor details'. The first field is 'Monitor name' with the text 'Auth Successes' entered. The second section is 'Monitor type', which contains four radio button options: 'Per query monitor' (selected), 'Per bucket monitor', 'Per document monitor', and 'Composite monitor'. Each option has a brief description. The third section is 'Monitor defining method', with the instruction 'Specify the way you want to define your query and triggers. [Learn more](#)'. It contains two radio button options: 'Visual editor' (selected) and 'Extraction query editor'. The final section is 'Schedule', with a 'Frequency' label and a dropdown menu.

W. Alerting Monitors Create monitor

Create monitor

Monitor details

Monitor name

Auth Successes

Monitor type

☒ **Per query monitor**
Per query monitors run a query and generate alerts based on trigger criteria that match query results.

☐ **Per bucket monitor**
Per bucket monitors run a query and generate alerts based on trigger criteria based on the dataset.

☐ **Per document monitor**
Per document monitors run queries that return individual documents matching the trigger conditions.

☐ **Composite monitor**
Composite monitors combine different monitor types and conditions to reduce alert noise and provide finer results.

Monitor defining method
Specify the way you want to define your query and triggers. [Learn more](#)

☒ **Visual editor**

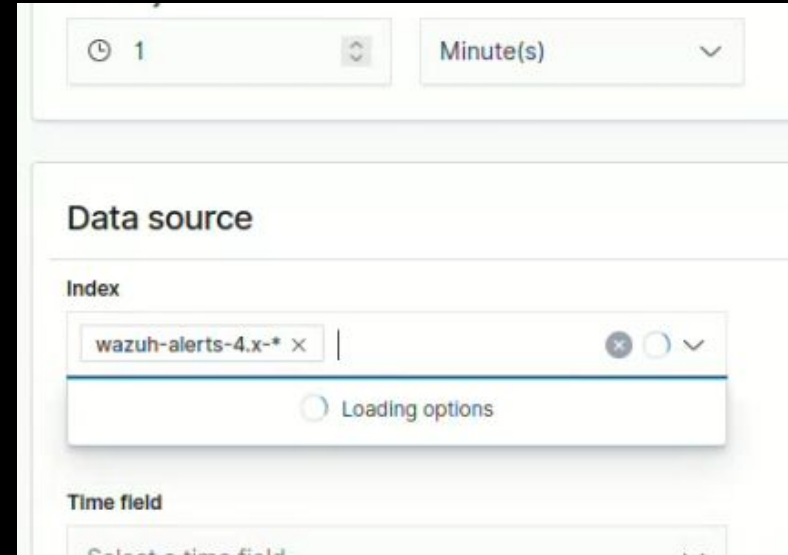
☐ **Extraction query editor**

Schedule

Frequency

Tour: Creating an Alert (4/9)

Type “wazuh-alerts-4.x-*” as a data source.



The screenshot shows a configuration interface for creating an alert. At the top, there is a time range selector set to '1' minute(s). Below this, the 'Data source' section is visible. Under the 'Index' label, a text input field contains 'wazuh-alerts-4.x-*'. Below the input field, there is a dropdown menu with the text 'Loading options'. The 'Time field' section is partially visible at the bottom.

Tour: Creating an Alert (5/9)

Create a filter to only show
“authentication_success” events.

The screenshot displays the 'Query' configuration section of a dashboard. It includes a 'Metrics' section with a 'COUNT OF documents' metric and an 'Add metric' button. Below this is a 'Time range for the last' section with a value of '1' and a unit of 'hour(s)'. The 'Data filter' section shows a filter for 'rule.groups is authentication_success'. An 'ADD DATA FILTER' modal is open, showing a dropdown for 'rule.groups', a dropdown for 'is', and a text input for 'authentication_success'. At the bottom, there is a link to 'Preview query and performance'.

Query

Metrics - optional ⓘ

COUNT OF documents

+ Add metric

You can add up to 1 metric.

Time range for the last ⓘ

1 hour(s)

Data filter - optional ⓘ

rule.groups is authentication_success ×

ADD DATA FILTER

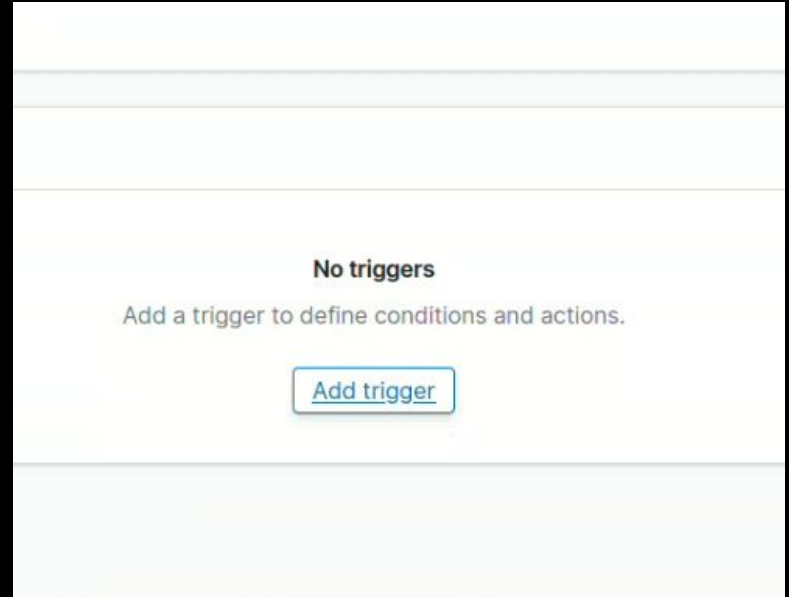
rule.groups is authentication_success

You can add up to 1 group by.

> Preview query and performance

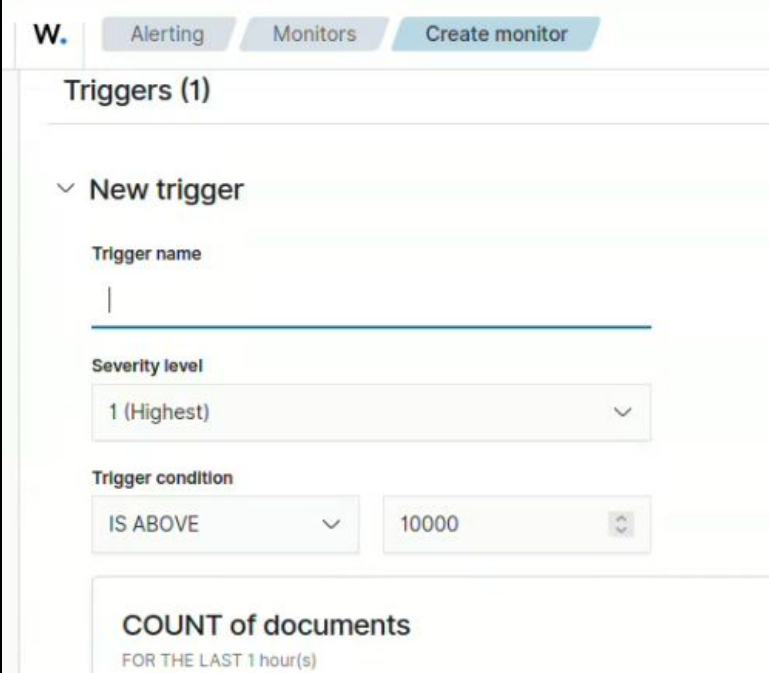
Tour: Creating an Alert (6/9)

Click “Add trigger”.



Tour: Creating an Alert (7/9)

Name the new trigger you just created.



The screenshot shows a web interface for creating a monitor. At the top, there are three tabs: 'Alerting', 'Monitors', and 'Create monitor'. The 'Create monitor' tab is active. Below the tabs, the title 'Triggers (1)' is displayed. A section titled 'New trigger' is expanded, showing the following fields:

- Trigger name:** A text input field with a vertical cursor.
- Severity level:** A dropdown menu currently set to '1 (Highest)'.
- Trigger condition:** A dropdown menu set to 'IS ABOVE'.
- Value:** A text input field containing the number '10000'.

Below these fields, the text 'COUNT of documents' is displayed, followed by 'FOR THE LAST 1 hour(s)'.

Tour: Creating an Alert (8/9)

Set the detection threshold for the trigger.

Triggers (1)

Unusually many successful logins

Trigger name

Unusually many successful logins

Severity level

1 (Highest)

Trigger condition

IS ABOVE

12

COUNT of documents

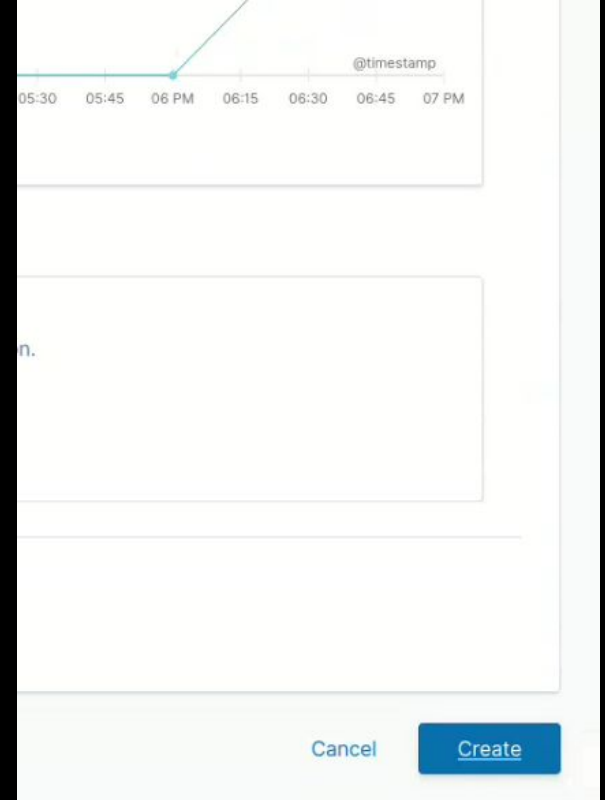
FOR THE LAST 1 hour(s)

22

count

Tour: Creating an Alert (9/9)

Click “Create”.



The screenshot shows a web interface for creating an alert. At the top, there is a horizontal timeline with tick marks and labels: 05:30, 05:45, 06 PM, 06:15, 06:30, 06:45, and 07 PM. A teal line is plotted on the timeline, starting from the left and ending at a point labeled "06 PM". A small teal dot is at the end of this line. To the right of the timeline, the text "@timestamp" is visible. Below the timeline is a large, empty rectangular input field. At the bottom right of the form, there are two buttons: a "Cancel" button and a blue "Create" button.