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.

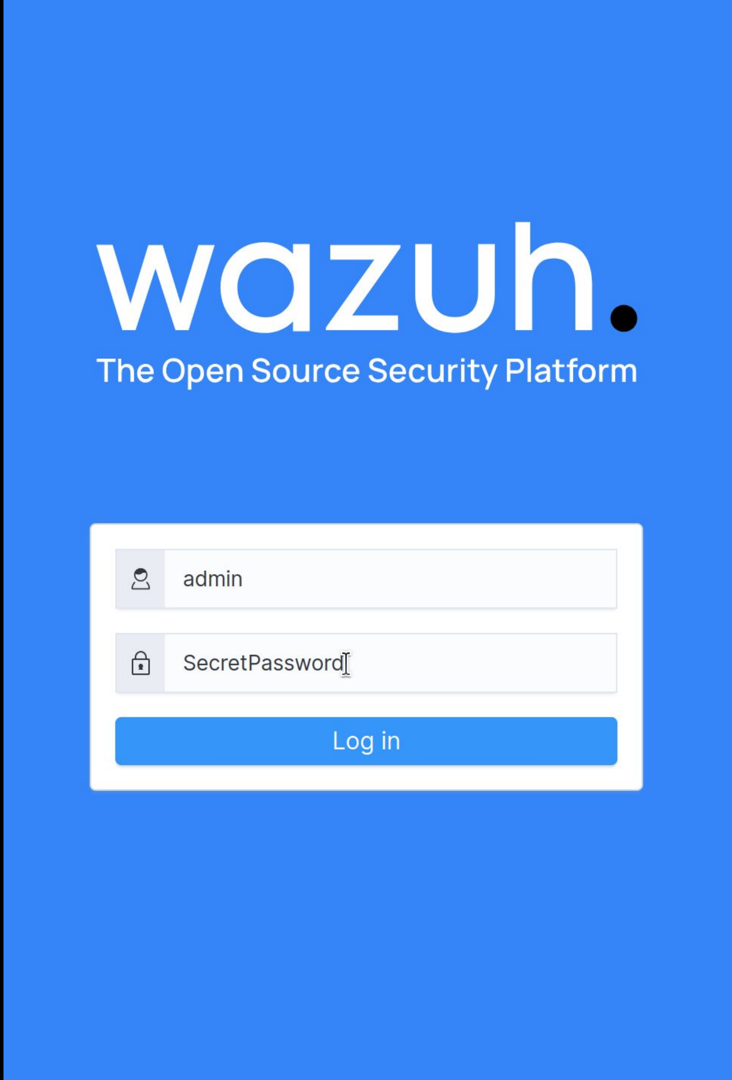
Installing the Wazuh agent

- `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`



admin

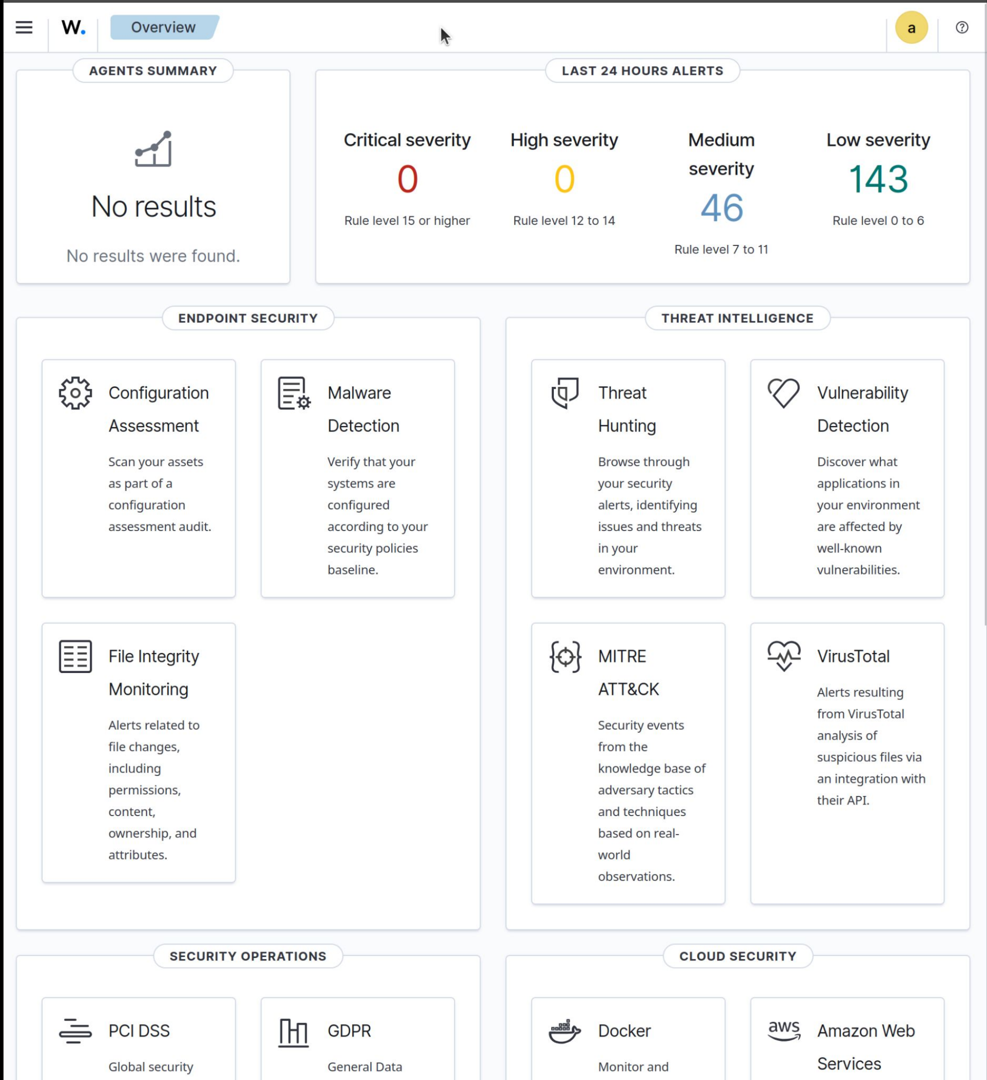
SecretPassword

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)



AGENTS SUMMARY

No results

No results were found.

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	46	143
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment

Scan your assets as part of a configuration assessment audit.

Malware Detection

Verify that your systems are configured according to your security policies baseline.

File Integrity Monitoring

Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting

Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection

Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK

Security events from the knowledge base of adversary tactics and techniques based on real-world observations.

VirusTotal

Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.

SECURITY OPERATIONS

PCI DSS

Global security

GDPR

General Data

CLOUD SECURITY

Docker

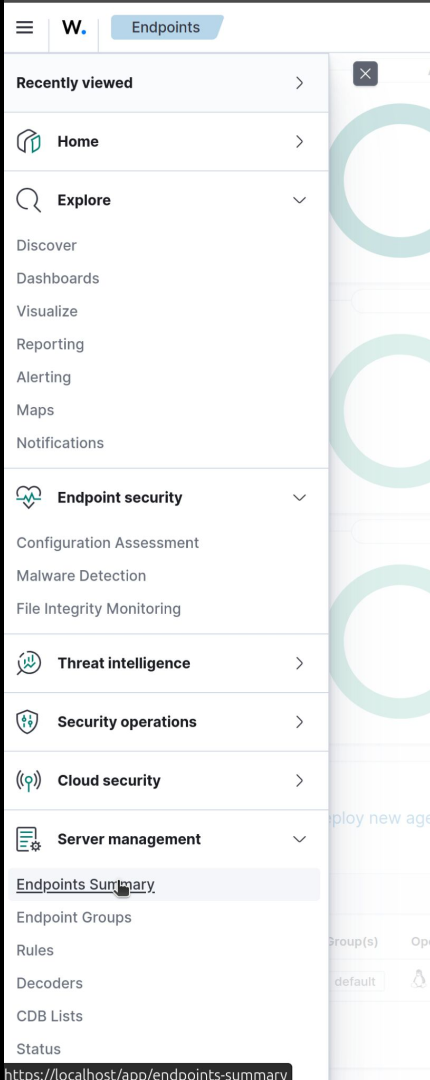
Monitor and

Amazon Web Services

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.

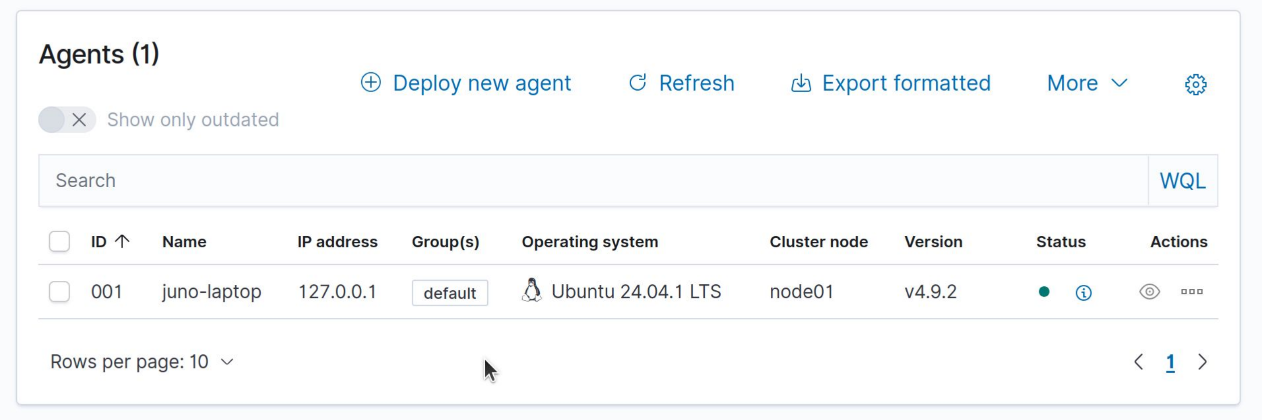
Let’s go to “**Endpoints Summary**” in the “Server management” section to make sure the Wazuh agent you installed earlier is connected.



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)

□	ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
□	001	juno-laptop	127.0.0.1	default	Ubuntu 24.04.1 LTS	node01	v4.9.2	●	

Tour: Explore Tab

We will focus on the following in this lab:

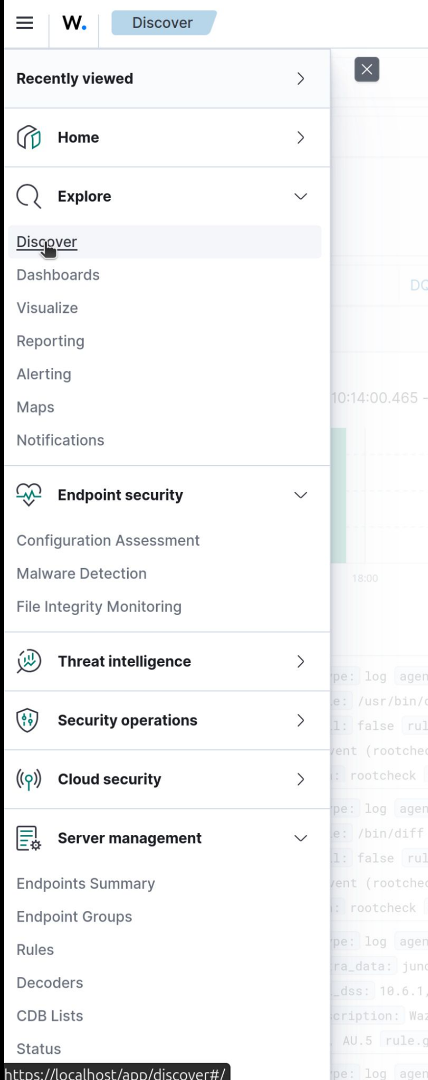
Discover: Manually filter and view events.

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.

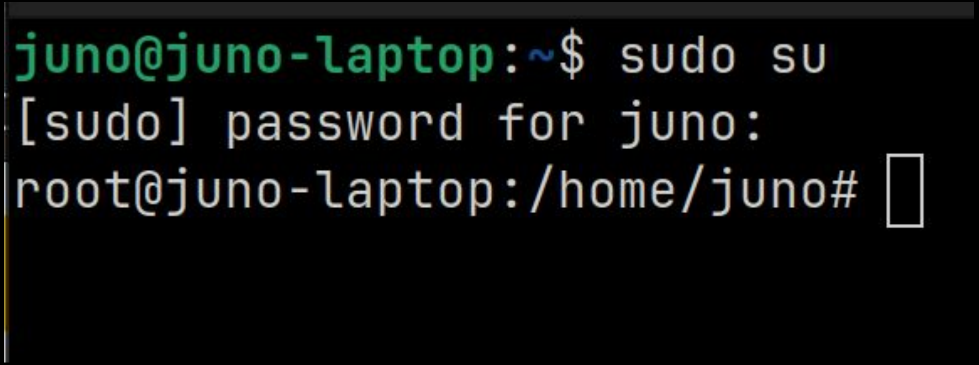


Tour: Generate some events

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.

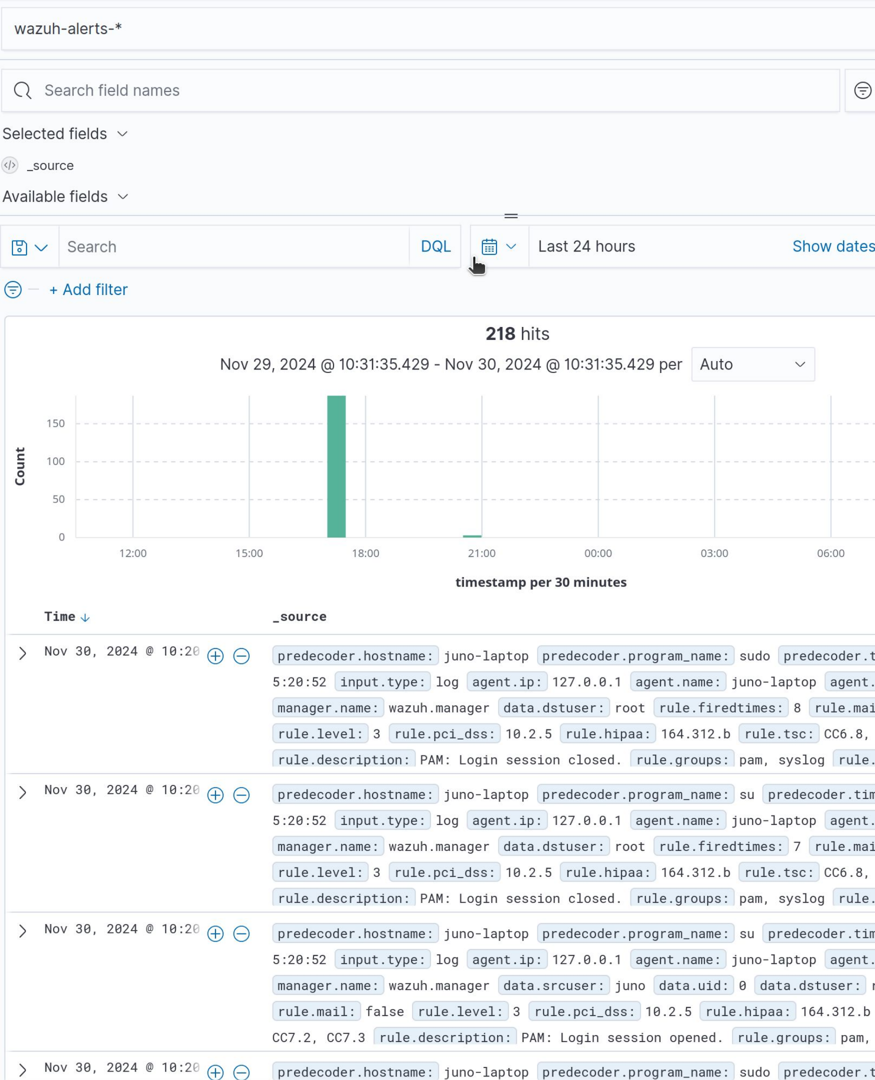


```
juno@juno-laptop:~$ sudo su
[sudo] password for juno:
root@juno-laptop:/home/juno#
```

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.



218 hits

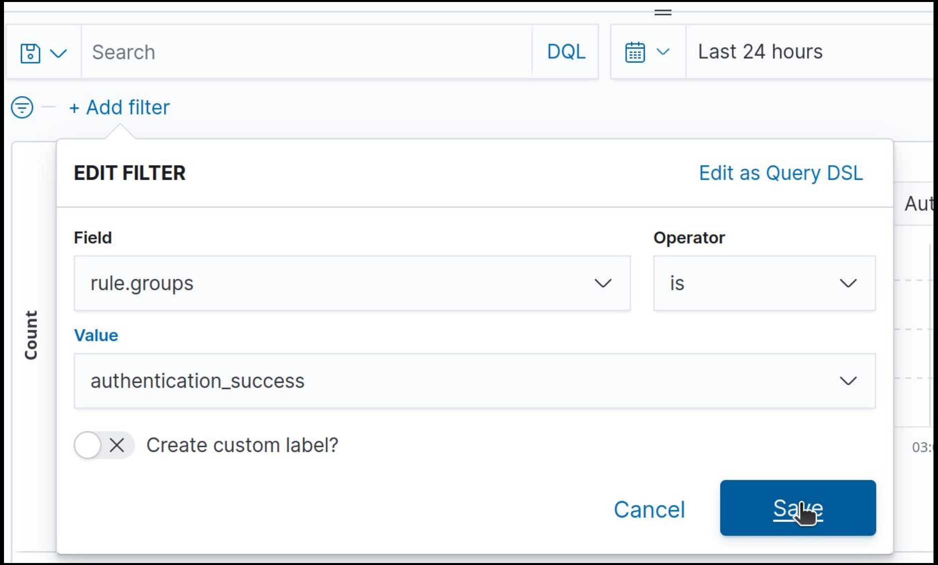
Nov 29, 2024 @ 10:31:35.429 - Nov 30, 2024 @ 10:31:35.429 per Auto

```
Nov 30, 2024 @ 10:20   predecoder.hostname: juno-laptop predecoder.program_name: sudo predecoder.t
                       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   predecoder.hostname: juno-laptop predecoder.program_name: su predecoder.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   predecoder.hostname: juno-laptop predecoder.program_name: su predecoder.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   predecoder.hostname: juno-laptop predecoder.program_name: sudo predecoder.t
```

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.



EDIT FILTER

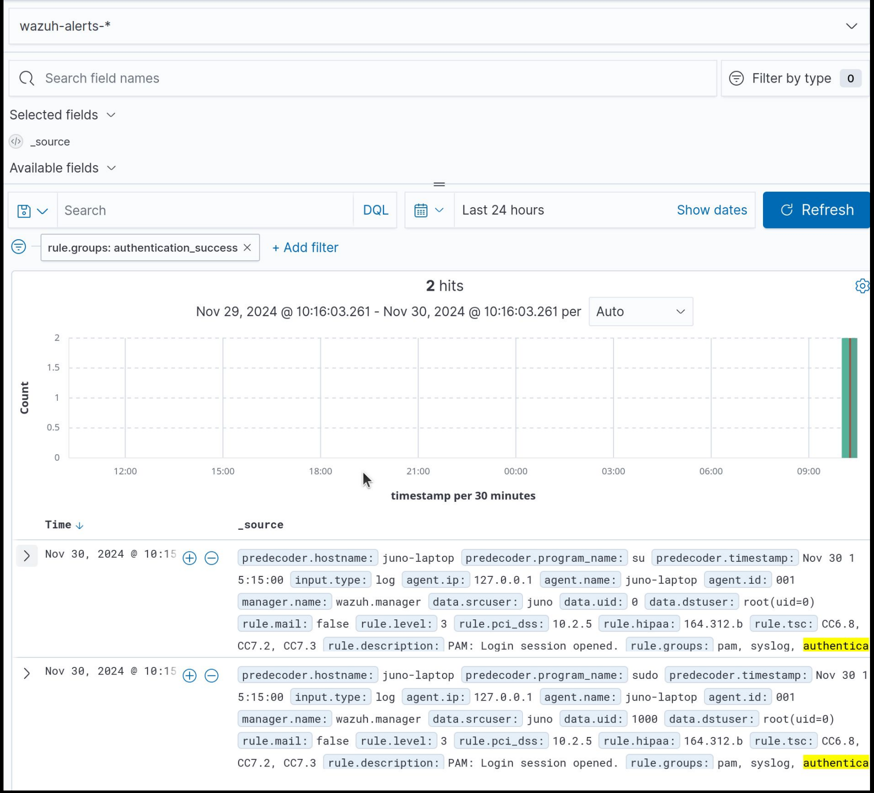
Field: rule.groups

Operator: is

Value: authentication_success

Tour: Using Discover

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



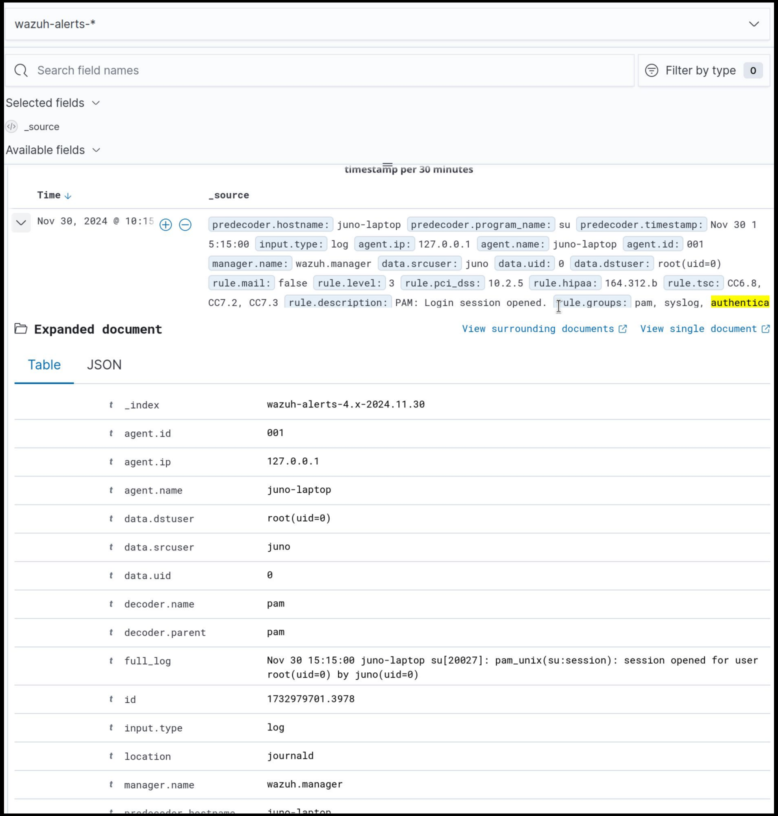
2 hits

Nov 29, 2024 @ 10:16:03.261 - Nov 30, 2024 @ 10:16:03.261 per Auto

```
Nov 30, 2024 @ 10:15   predecoder.hostname: juno-laptop predecoder.program_name: su predecoder.timestamp: Nov 30 1
                       5:15:00 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, authentica
Nov 30, 2024 @ 10:15   predecoder.hostname: juno-laptop predecoder.program_name: sudo predecoder.timestamp: Nov 30 1
                       5:15:00 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: 1000 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, authentica
```

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 ↓	_source
Nov 30, 2024 @ 10:15	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, authentica

Expanded document

View surrounding documents

View single document

Table JSON

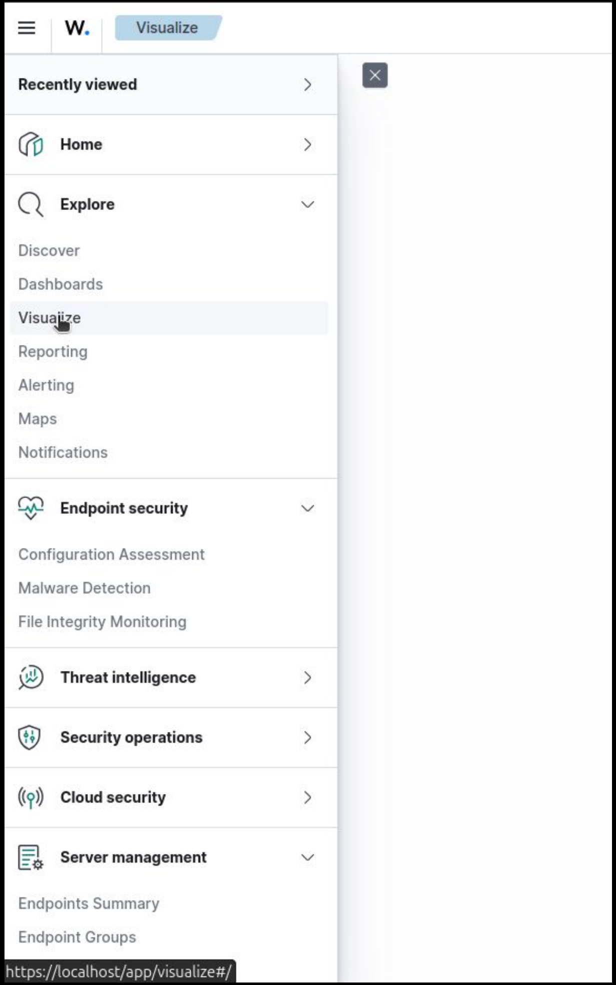
t	_index	wazuh-alerts-4.x-2024.11.30
t	agent.id	001
t	agent.ip	127.0.0.1
t	agent.name	juno-laptop
t	data.dstuser	root(uid=0)
t	data.srcuser	juno
t	data.uid	0
t	decoder.name	pam
t	decoder.parent	pam
t	full_log	Nov 30 15:15:00 juno-laptop su[20027]: pam_unix(su:session): session opened for user root(uid=0) by juno(uid=0)
t	id	1732979701.3978
t	input.type	log
t	location	journald
t	manager.name	wazuh.manager
t	predecoder.hostname	juno-laptop

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

Tour:
Creating a Chart

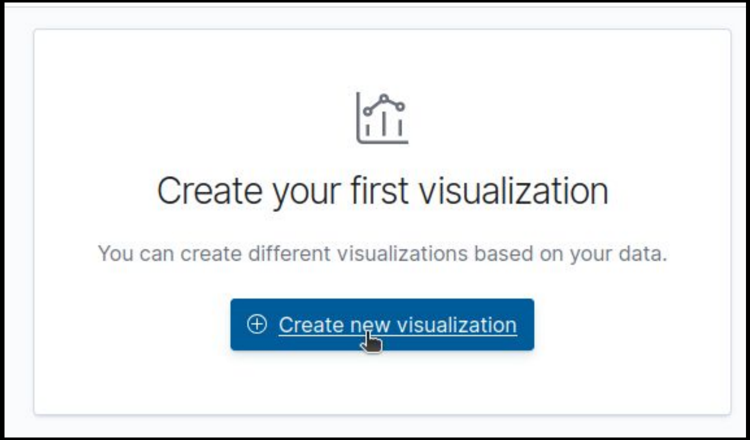
Tour: Creating a Chart (1/12)

In the sidebar, click “Visualize”.



Tour: Creating a Chart (2/12)

Click “Create new visualization”.



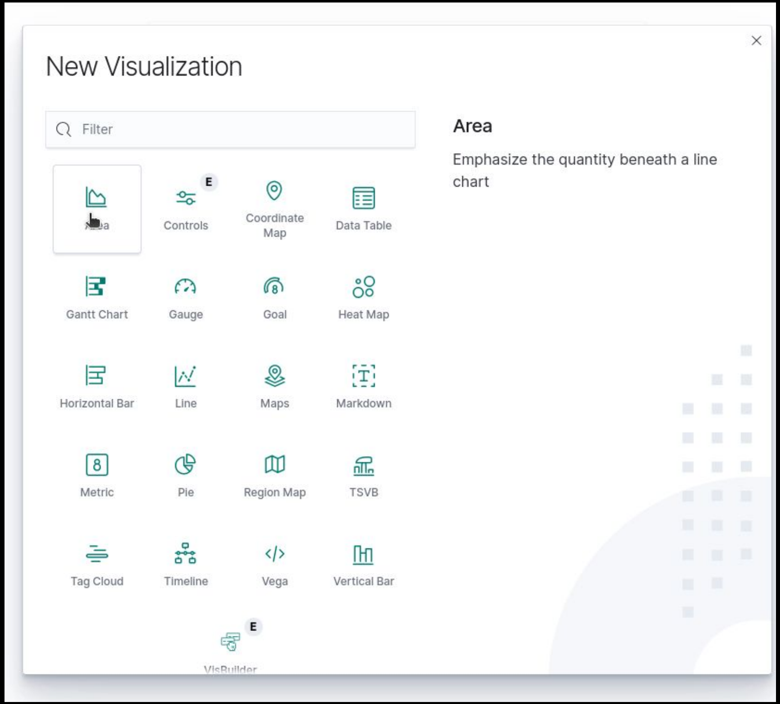
Create your first visualization

You can create different visualizations based on your data.

Tour: Creating a Chart (3/12)

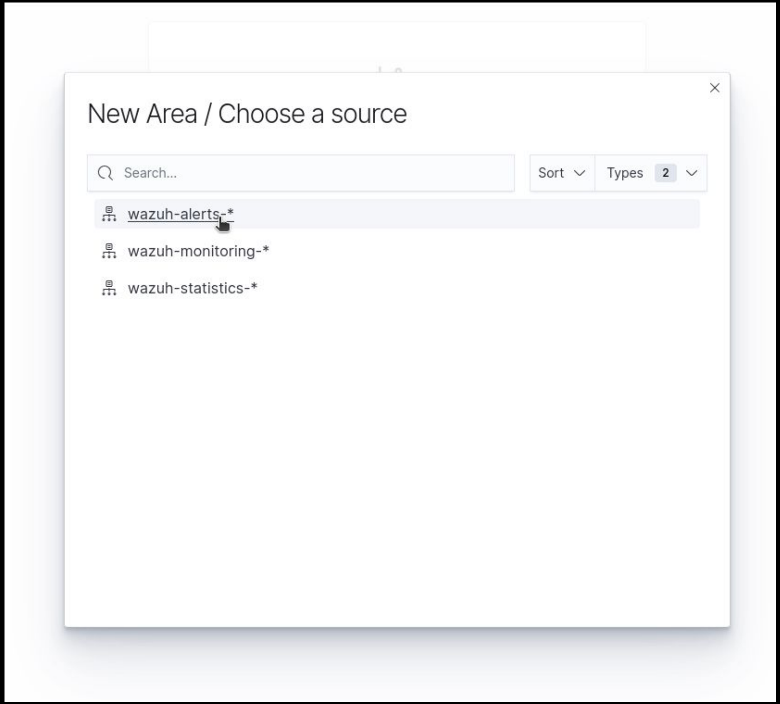
Click “Area”.

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



Tour: Creating a Chart (4/12)

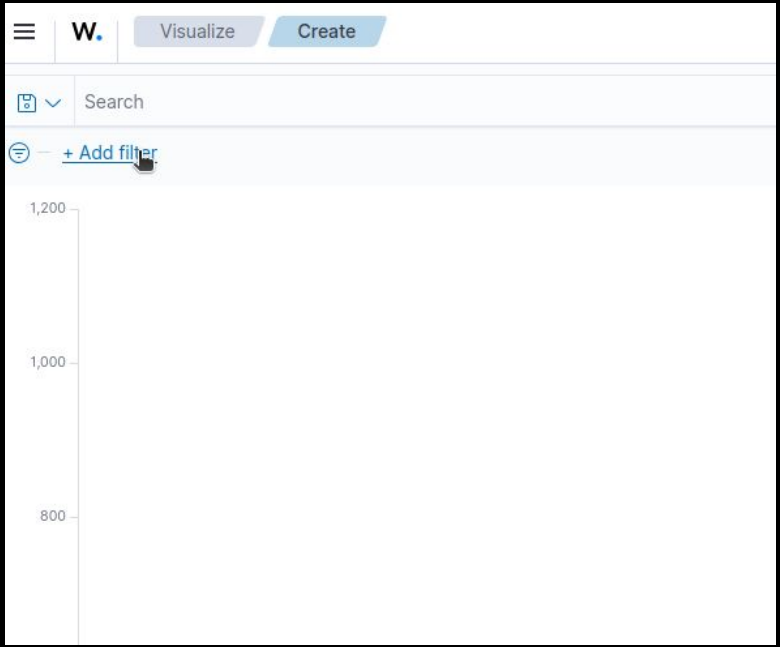
Click “wazuh-alerts-*”.



Tour: Creating a Chart (5/12)

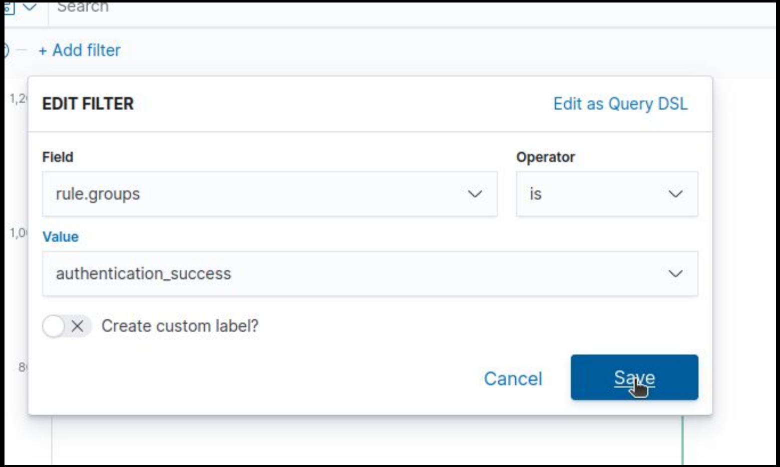
Now you’re ready to create the chart.

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”.



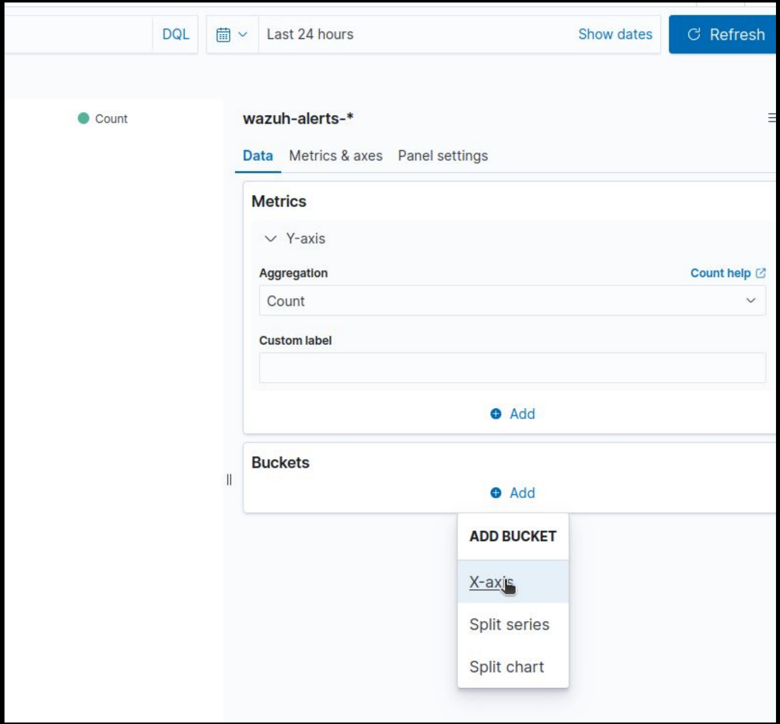
Field: rule.groups

Operator: is

Value: authentication_success

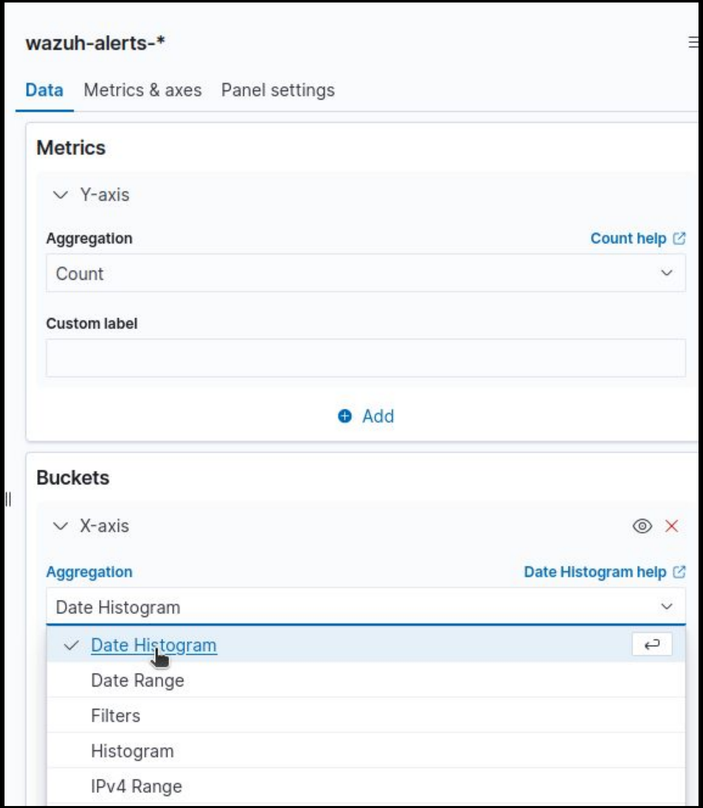
Tour: Creating a Chart (7/12)

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”.


wazuh-alerts-*

Metrics

Y-axis

Aggregation: Count

Custom label

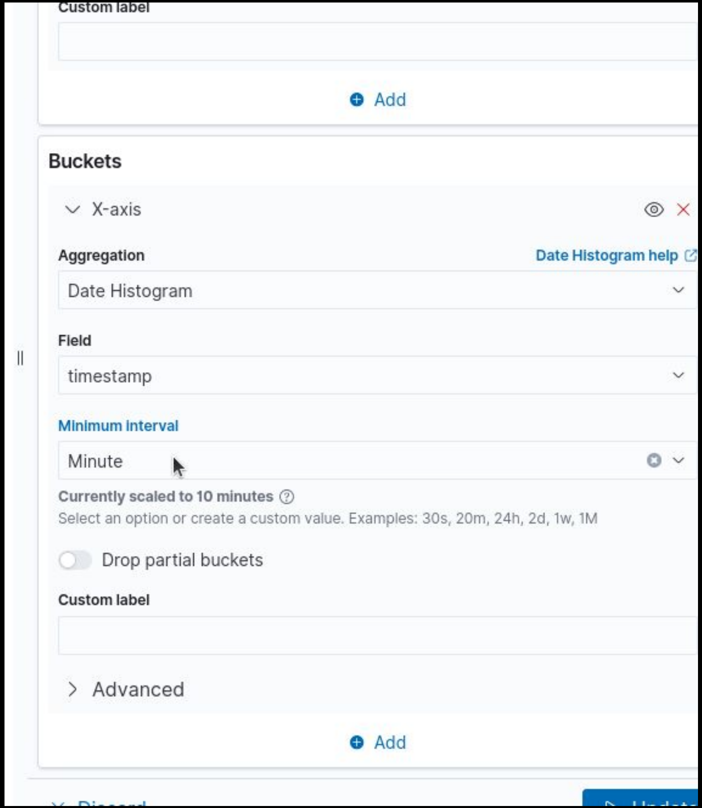
Buckets

X-axis

Aggregation: Date Histogram

Tour: Creating a Chart (9/12)

For the minimum interval, select “Minute”.



Custom label

Aggregation: Date Histogram

Field: timestamp

Minimum interval: Minute

Currently scaled to 10 minutes

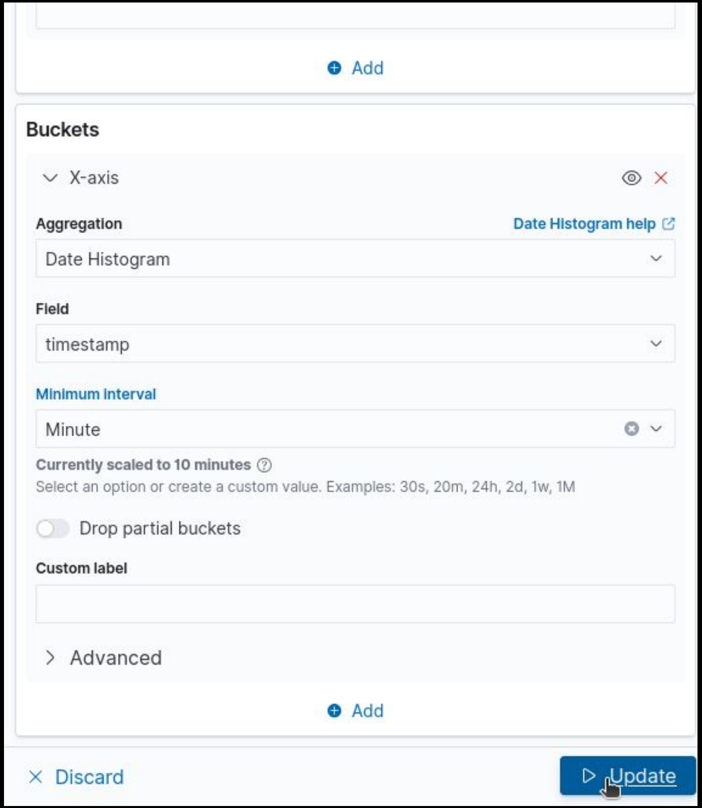
Select an option or create a custom value. Examples: 30s, 20m, 24h, 2d, 1w, 1M

Drop partial buckets

Custom label

Tour: Creating a Chart (10/12)

Click “Update” to see the chart.



Buckets

X-axis

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

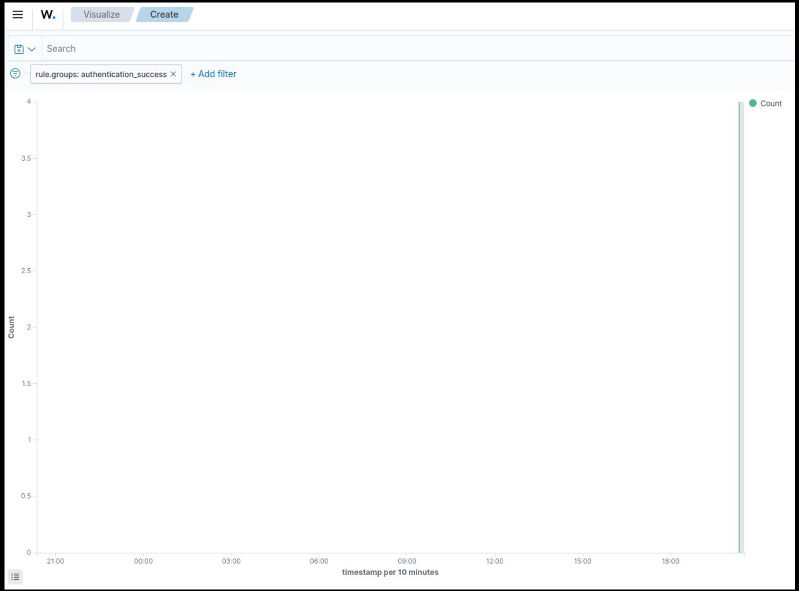
Drop partial buckets

Custom label

Tour: Creating a Chart (11/12)

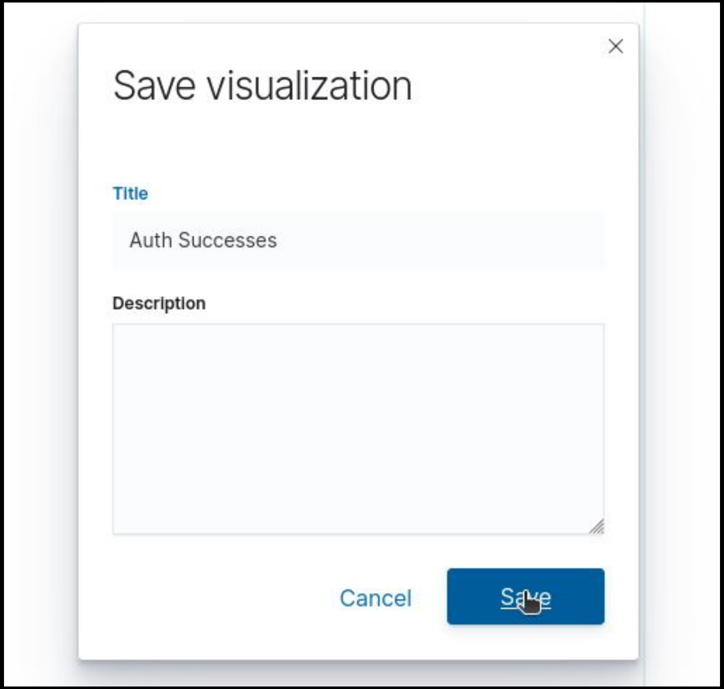
You should see a chart showing successful login attempts.

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



Tour: Creating a Chart (12/12)

Name the visualization and click “Save”.



Save visualization

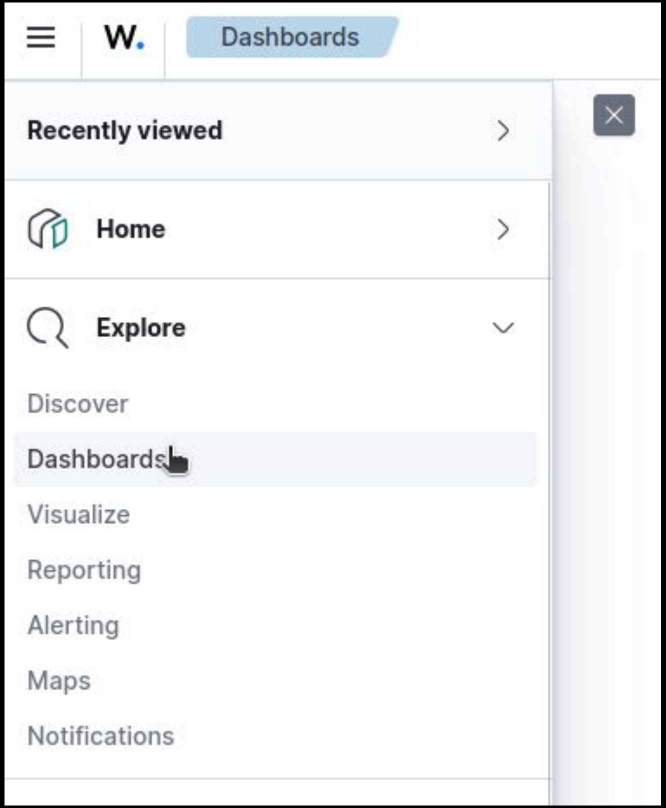
Title: Auth Successes

Description:

Tour:
Creating a Dashboard

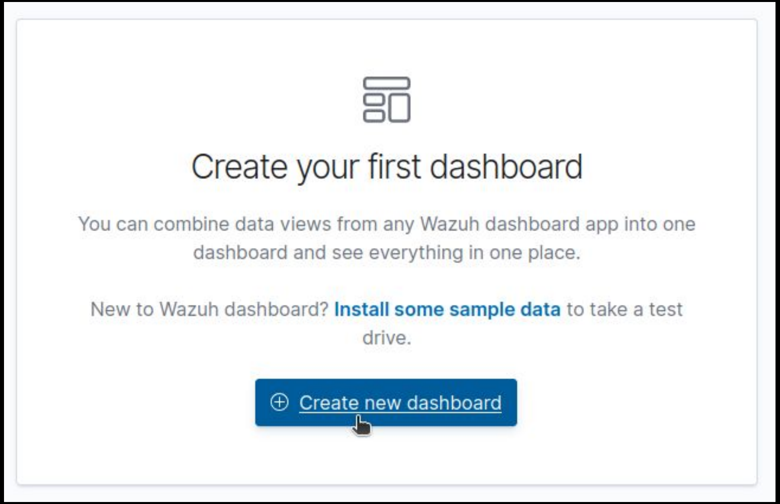
Tour: Creating a Dashboard (1/6)

Click “Dashboards” in the sidebar.



Tour: Creating a Dashboard (2/6)

Click “Create new dashboard”.



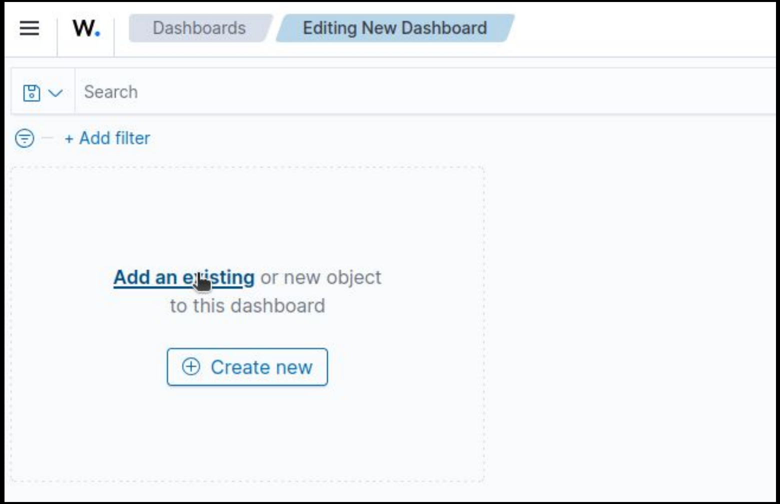
Create your first dashboard

You can combine data views from any Wazuh dashboard app into one dashboard and see everything in one place.

New to Wazuh dashboard? **Install some sample data** to take a test drive.

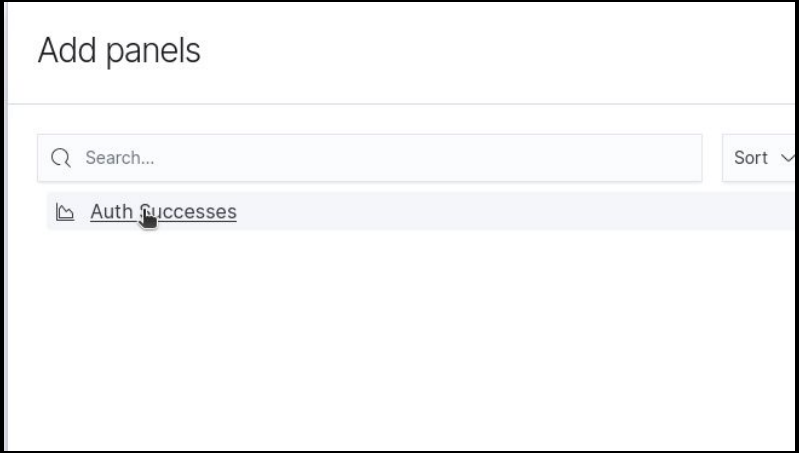
Tour: Creating a Dashboard (3/6)

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



Tour: Creating a Dashboard (4/6)

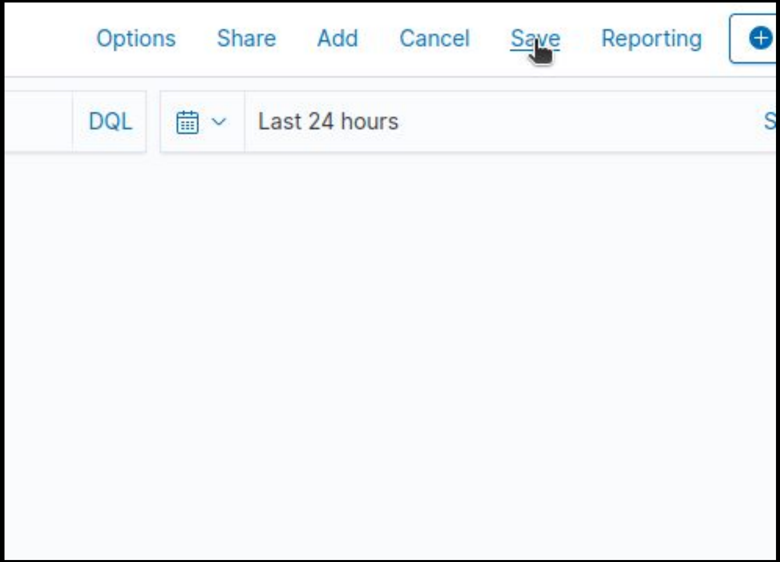
Click on the chart we created earlier.



Add panels

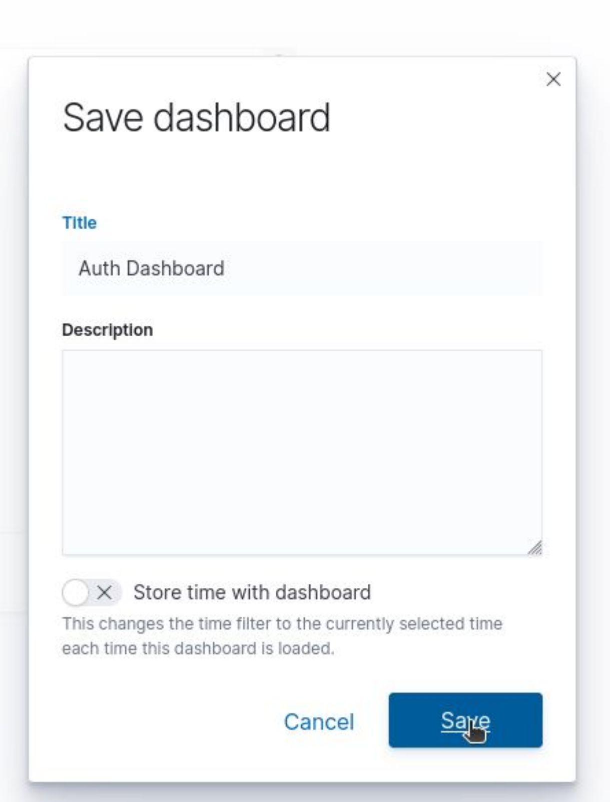
Tour: Creating a Dashboard (5/6)

Click “Save”.



Tour: Creating a Dashboard (6/6)

Fill in a name and click “Save”.



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.

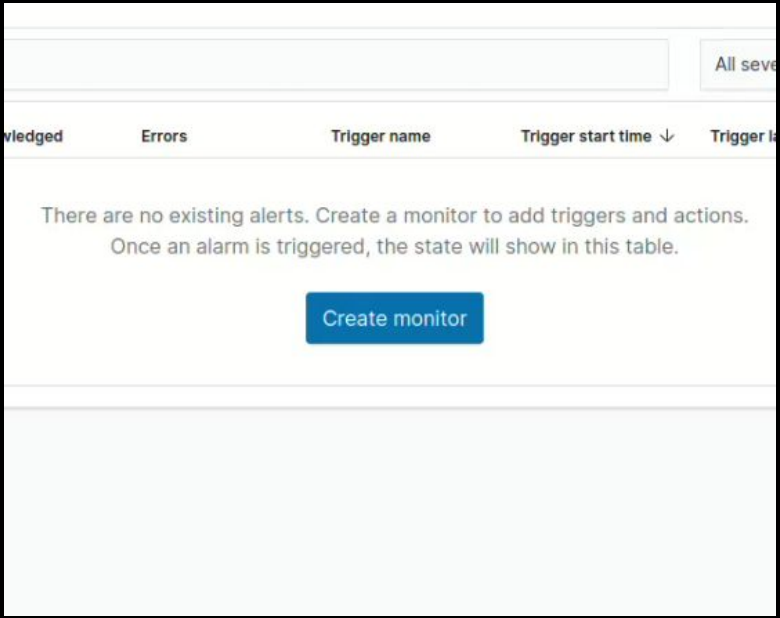
Tour:
Creating an Alert

Tour: Creating an Alert (1/9)

Navigate to “Alerting” in the sidebar.

Tour: Creating an Alert (2/9)

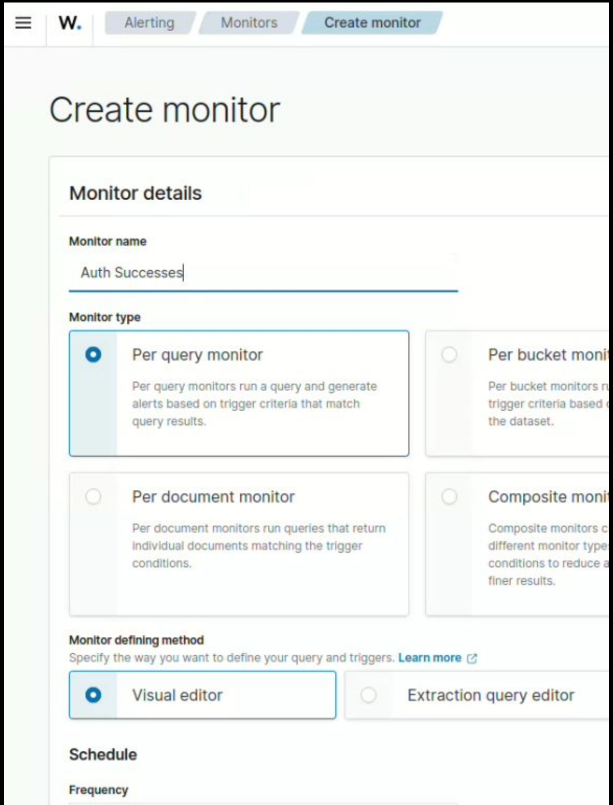
Click “Create Monitor”.



There are no existing alerts. Create a monitor to add triggers and actions.
Once an alarm is triggered, the state will show in this table.

Tour: Creating an Alert (3/9)

Fill in a name for the 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 moni

Per bucket monitors r trigger criteria based the dataset.

○ Per document monitor

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

○ Composite moni

Composite monitors c different monitor type conditions to reduce a finer results.

Monitor defining method

Specify the way you want to define your query and triggers. Learn more

● Visual editor

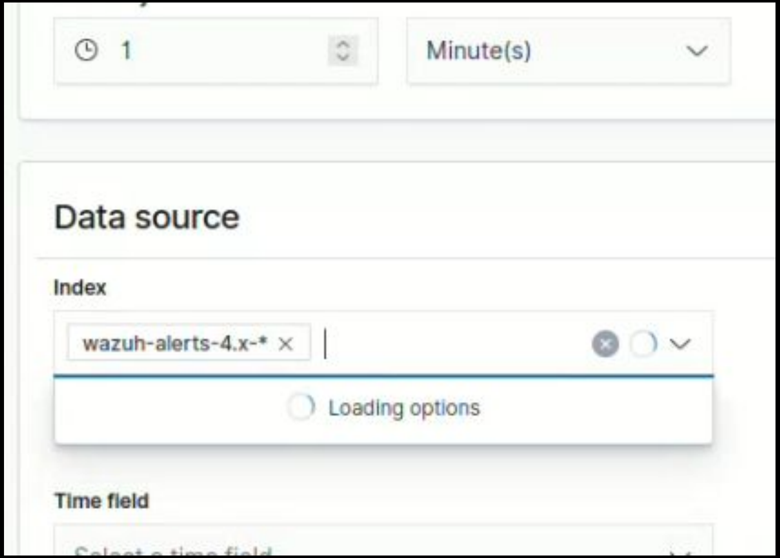
○ Extraction query editor

Schedule

Frequency

Tour: Creating an Alert (4/9)

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



1 Minute(s)

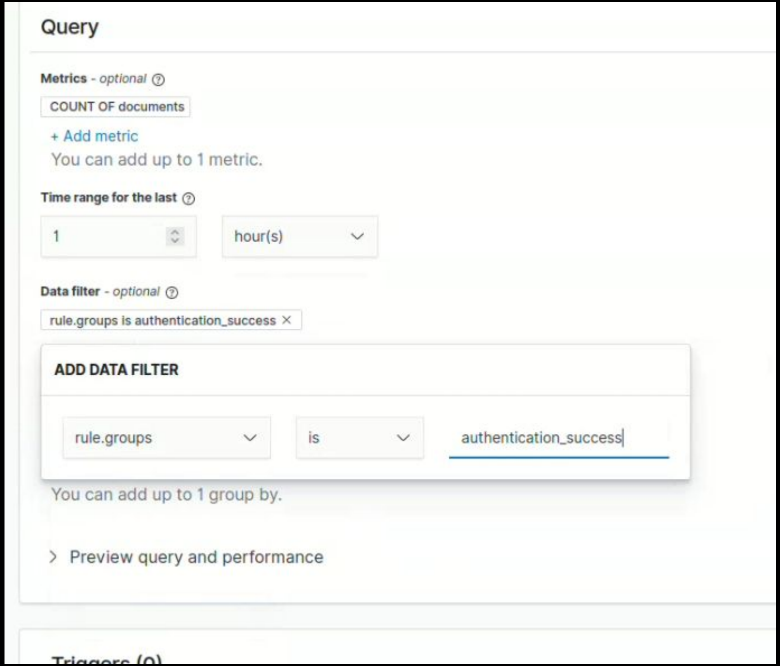
Data source

Index

wazuh-alerts-4.x-*

Tour: Creating an Alert (5/9)

Create a filter to only show “authentication_success” events.



Query

Metrics - *optional*

COUNT OF documents

You can add up to 1 metric.

Time range for the last: 1 hour(s)

Data filter - *optional*

rule.groups is authentication_success

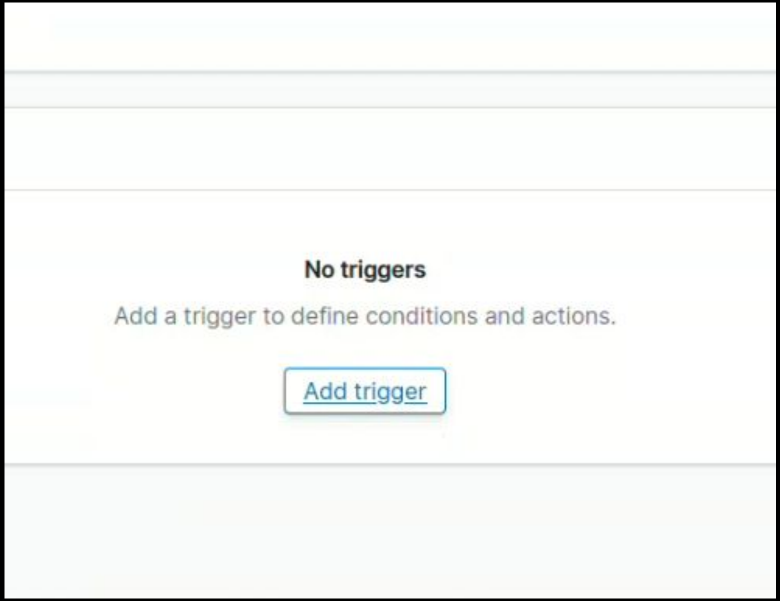
ADD DATA FILTER

rule.groups | is | authentication_success

You can add up to 1 group by.

Tour: Creating an Alert (6/9)

Click “Add trigger”.

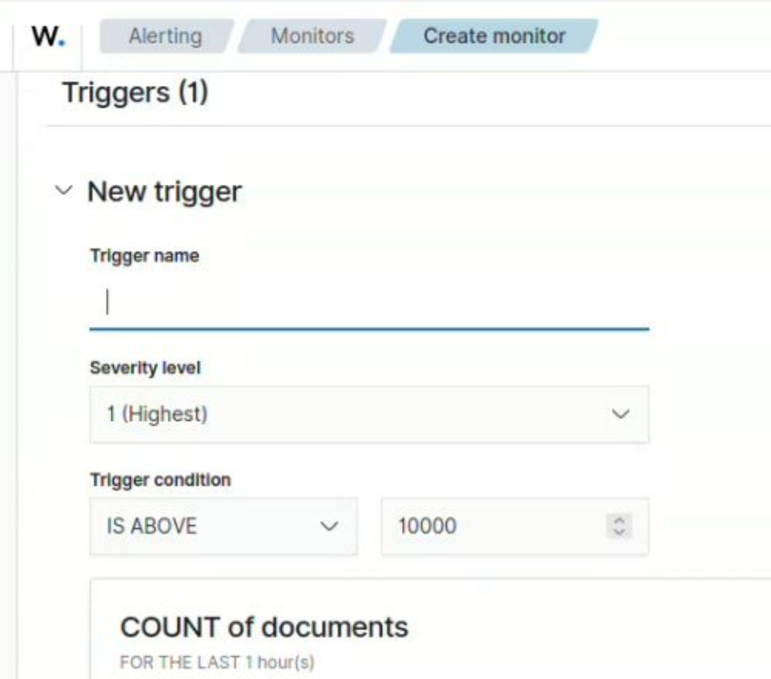


No triggers

Add a trigger to define conditions and actions.

Tour: Creating an Alert (7/9)

Name the new trigger you just created.



Triggers (1)

New trigger

Trigger name

Severity level: 1 (Highest)

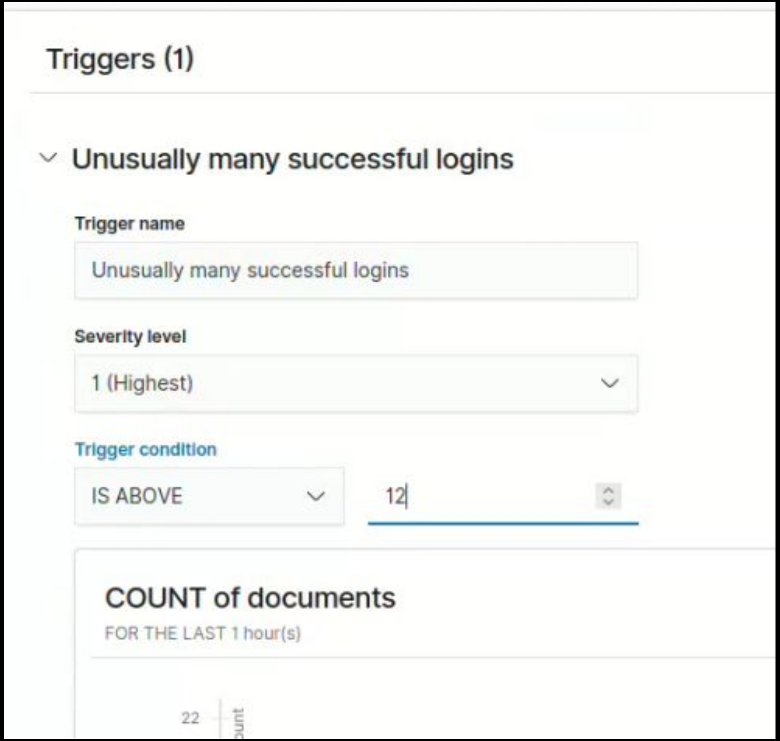
Trigger condition: IS ABOVE 10000

COUNT of documents

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)

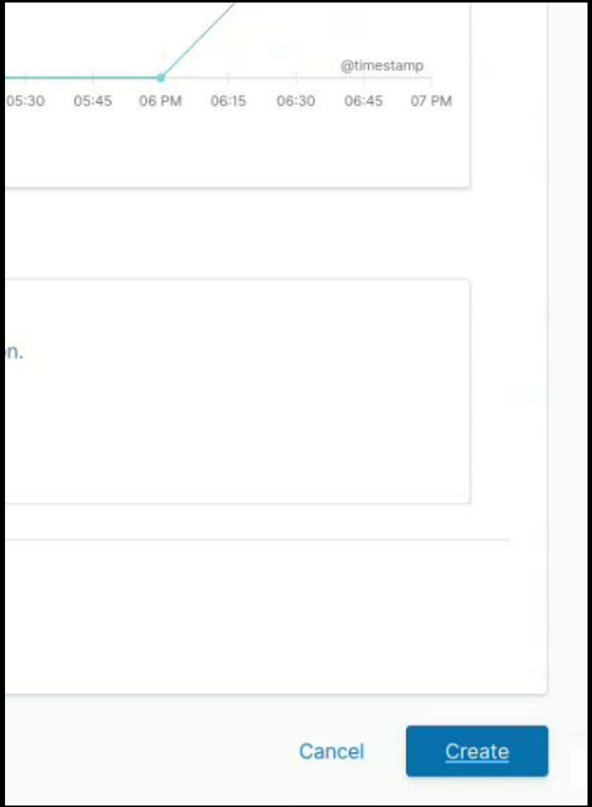
Trigger condition: IS ABOVE 12

COUNT of documents

FOR THE LAST 1 hour(s)

Tour: Creating an Alert (9/9)

Click “Create”.


@timestamp
05:30
05:45
06 PM
06:15
06:30
06:45
07 PM
n.
Cancel
Create