



WAZUH



Grafana

## Mod:37

### Grafana Creating Visualization, Dashboard and Integrated Wazuh

Grafana is a powerful **open-source analytics and visualization platform** used to monitor and visualize metrics from various data sources in real time.

#### What Grafana Does

Grafana helps you:

- **Visualize** data using interactive graphs, charts, and dashboards.
- **Monitor** infrastructure, applications, and services.
- **Alert** on anomalies and thresholds (e.g., high CPU usage).
- **Query** multiple data sources (like Aws, Elasticsearch, etc.).

#### Data Sources:

**Grafana connects to various backends like:**

- Prometheus
- InfluxDB
- Loki (logs)
- MySQL, PostgreSQL
- Elasticsearch
- AWS CloudWatch, Google Cloud, and more

#### Dashboards:

**Users create custom dashboards using panels that can:**

- Display time series (e.g., CPU over time)
- Show logs
- Visualize tables, pie charts, heatmaps, etc.

#### Alerts:

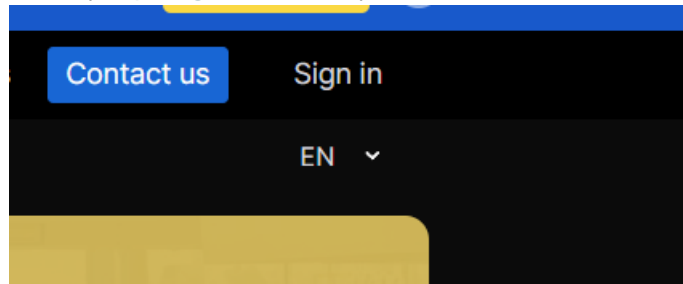
- Set alert conditions on graphs.
- Notify via Slack, email, Teams, PagerDuty, etc.

#### Plugins:

Grafana supports plugins to extend functionality — data sources, panels, and apps.

**Step:1** Create the account in official websites with your mail and create the password and and verify code in Gmail or outlook .

- Links:( <https://grafana.com/>)



**Step2:** Next install separated machine ubuntu or centos, rocky once setup and installation (Install the Grafana in ubuntu)

- <https://grafana.com/grafana/download> (Download Edition: OBB) Noted: Grafana Free-trail 15-days

Version: 11.6.1

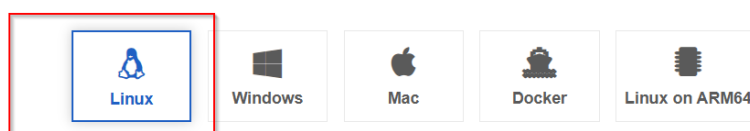
Edition: OSS

The [Enterprise Edition](#) is the default and recommended edition. It includes [Enterprise feature set](#), including support for [Enterprise plugins](#).

License: [AGPLv3](#)

Release Date: April 23, 2025

Release Info: [What's New In Grafana 11.6.1](#)



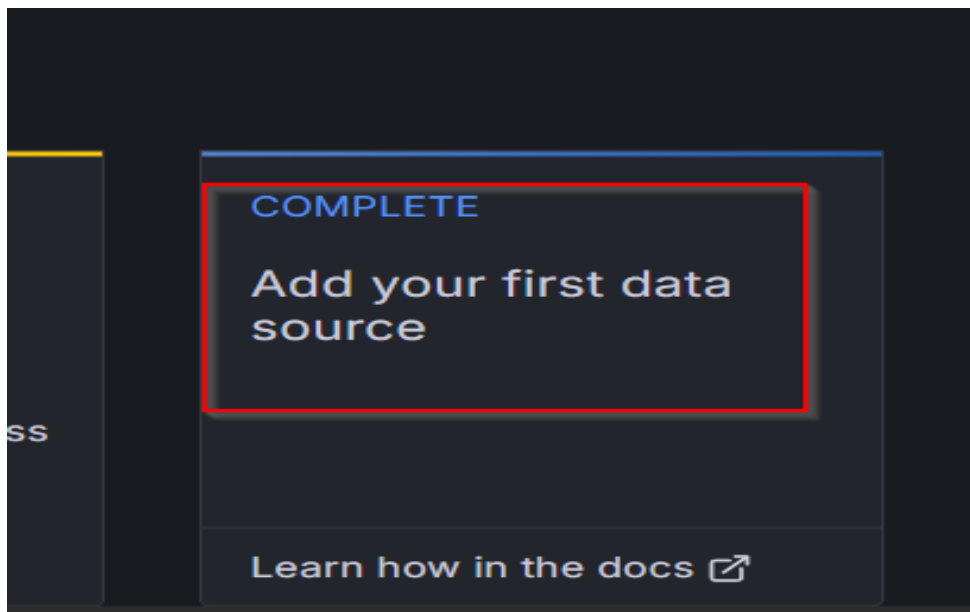
Ubuntu and Debian (64 Bit) SHA256: d644ad4d4cc4289a0d088063dca08ae2c36e5cb66817004ed026d513e6c85626

```
sudo apt-get install -y adduser libfontconfig1 musl
wget https://dl.grafana.com/oss/release/grafana_11.6.1_amd64.deb
sudo dpkg -i grafana_11.6.1_amd64.deb
```

Read the [Ubuntu / Debian installation guide](#) for more information. We also provide an [APT](#) package repository.

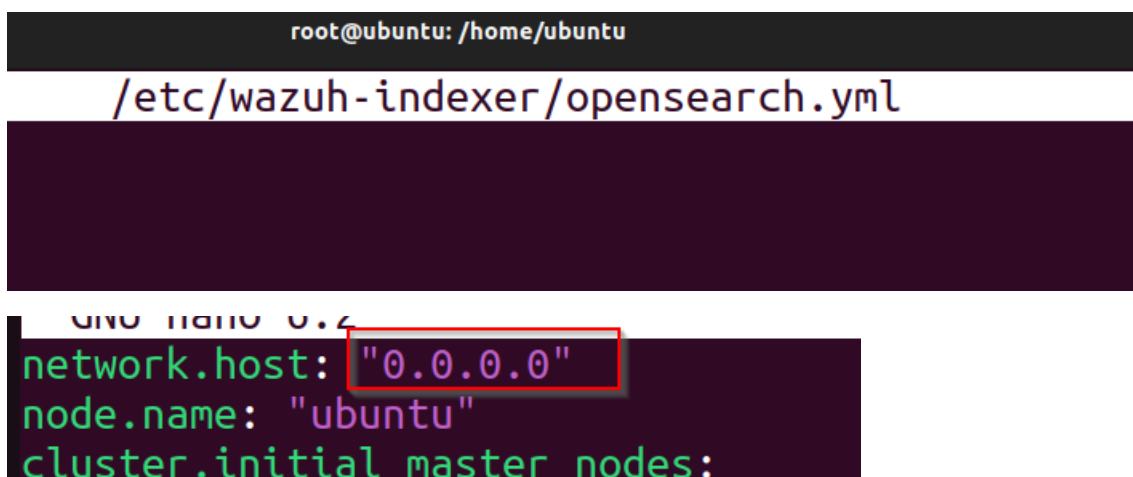
- Installtion it take time max 5 mins and once Grafana download start and enable the server (Systemctl enable Grafana-server and systemctl start Grafana-server) and next the status Grafana-server active or not ..
- Next check your ip address in machine go to browswer type the ip address with port 3000
- <http://192.168.1.1:3000> login page pop-up will open username and password admin and admin

- Once login there will user interface -Name called Data Sources click it and open



**Step3:** Navigate to Wazuh-server and set Wazuh-indexer bind ip address and because Grafana gonna monitoring entire of wazuh-alert messages and logs and give us visualization graphs

- Open with nano or vim editor /etc/wazuh-indexer/opensearch.yml

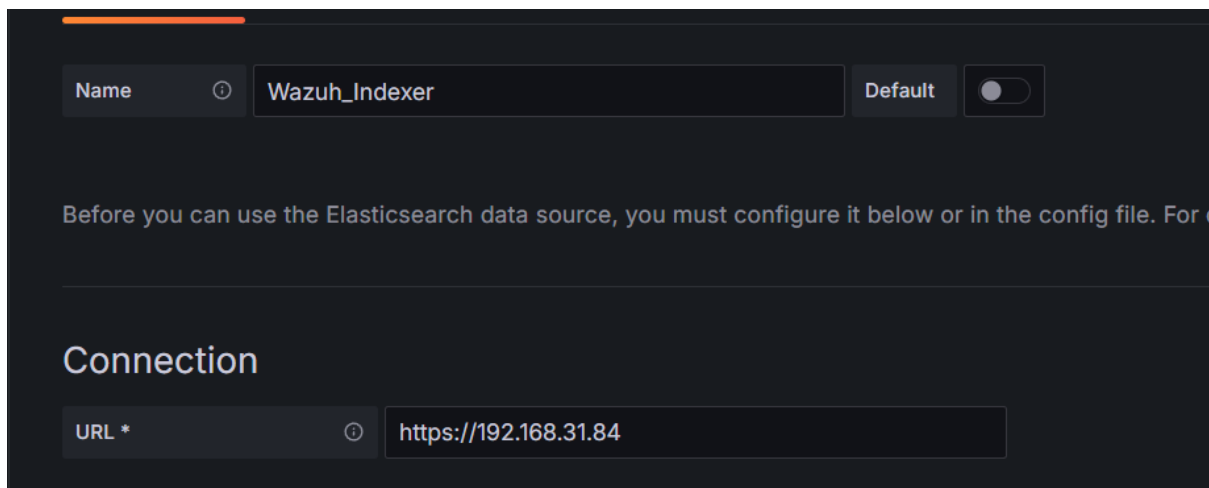
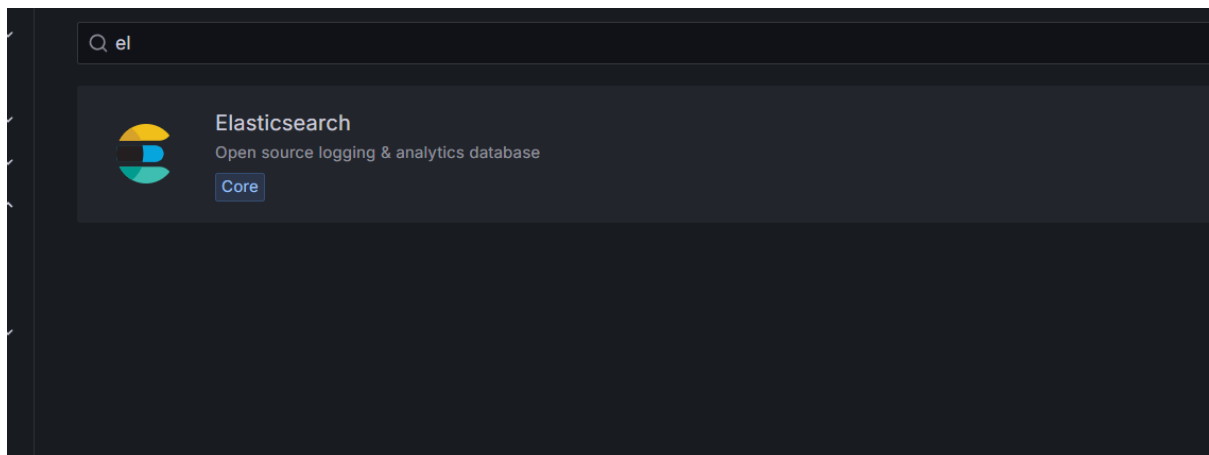


Above the images I have remove the previous Ip address and change to bind-address save and exit next,

- Systemctl restart wazuh-manager ,Systemctl restart wazuh-indexer, systemctl restart wazuh-dashboard

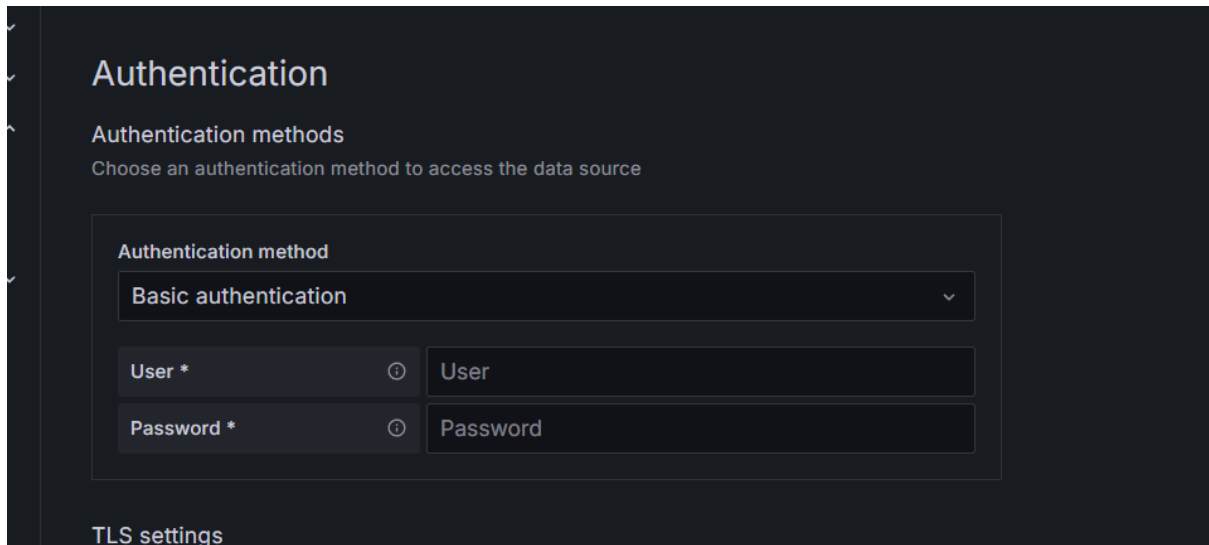
```
nano /etc/wazuh-indexer/opensearch.yml
systemctl restart wazuh-manager
systemctl restart wazuh-indexer
systemctl restart wazuh-dashboard
nano /etc/wazuh-indexer/opensearch.yml
```

**Step:4** Lets deploy in Grafana server go to add data source there will be search bar inside on ELASTICSEARCH and open the bar and we set the ip address of wazuh-server and some configuration.



Above the images I have rename the Wazuh\_indexer and connection set our wazuh-server ip address with 9200

**Step5:** In Authentication side change to Basic Authentication and add the username and password of Wazuh-Server



**Authentication**

Authentication methods  
Choose an authentication method to access the data source

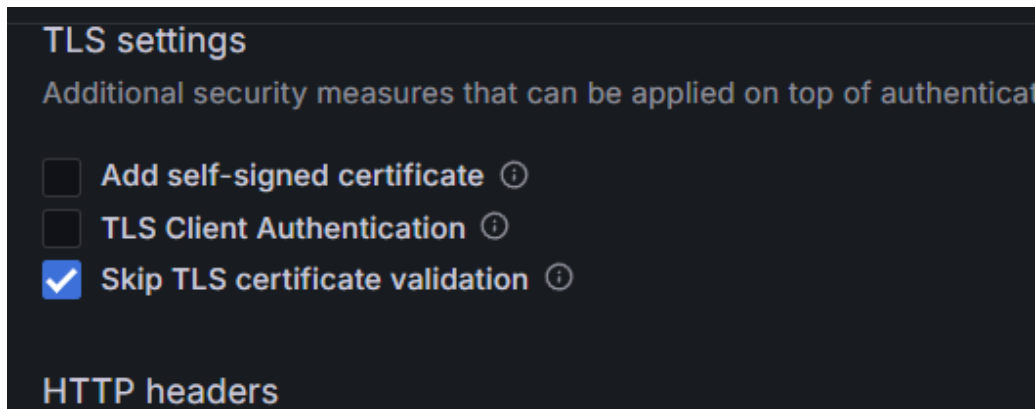
Authentication method  
Basic authentication

User \* User

Password \* Password

TLS settings

Next TLS Settings skip tls objections



**TLS settings**

Additional security measures that can be applied on top of authentication

☐ Add self-signed certificate

☐ TLS Client Authentication

☒ Skip TLS certificate validation

HTTP headers

**Step:6** Lets deploy add the wazuh-indexer and timestamp, rule.id, etc and next the SAVE and est config.

Specific settings for the Elasticsearch data source. [Learn more about Elasticsearch details](#)

Index name	ⓘ	wazuh-alerts-*
Pattern	ⓘ	No pattern
Time field name	ⓘ	timestamp
Max concurrent Shard Requests	ⓘ	5
Min time interval	ⓘ	10s
Include Frozen Indices	ⓘ	<input type="checkbox"/>

Logs

Configure which fields the data source uses for log messages and log levels. [Learn more about logs](#)

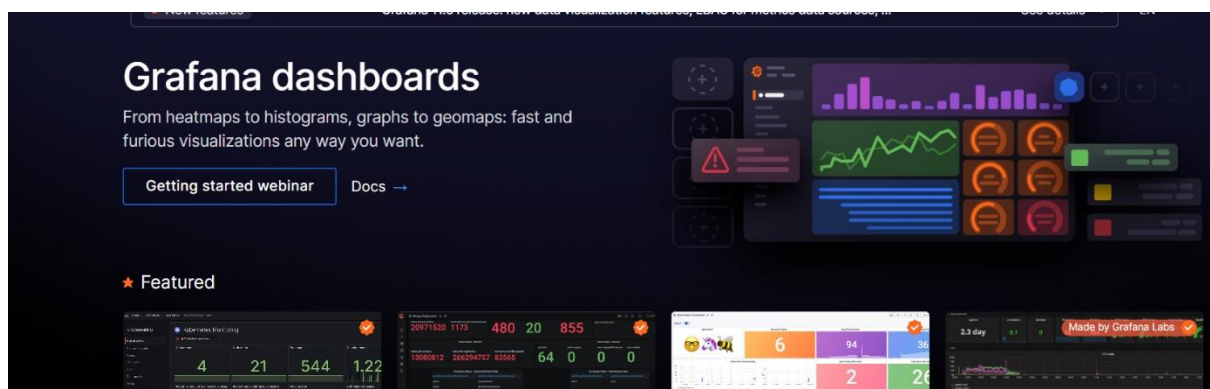
Message field name	ⓘ	rule.description
Level field name	ⓘ	rule.id

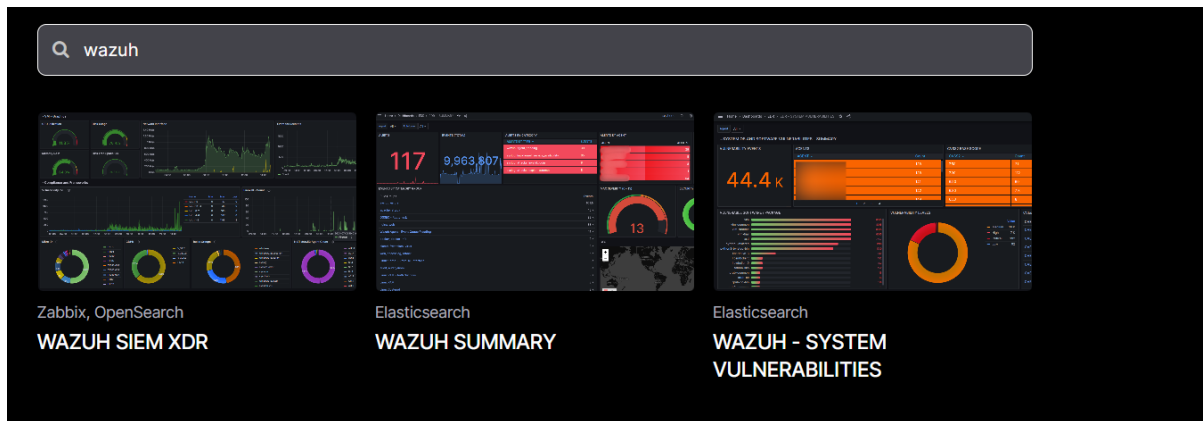
✓ Elasticsearch data source is healthy.

Next, you can start to visualize data by [building a dashboard](#), or by querying data in the [Explore view](#).

Above the images its success data source is healthy which it successfully connects to the wazuh-server.

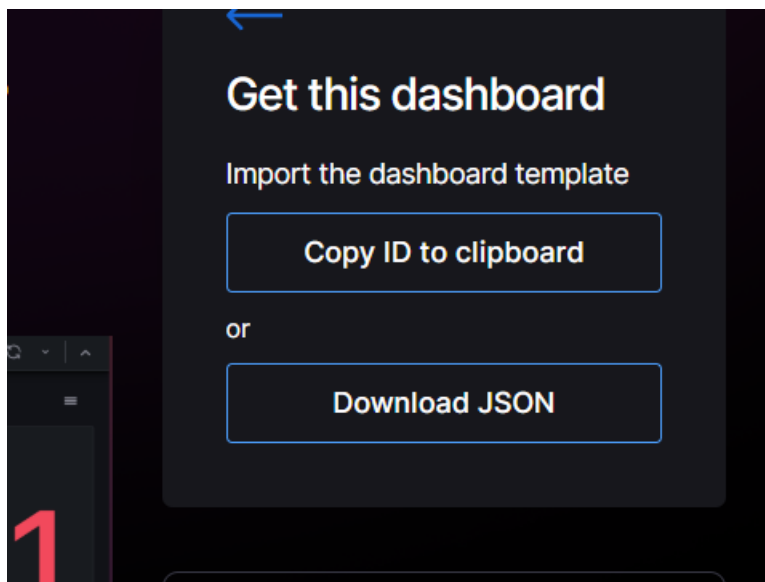
**Step7:** Next go to dashboard websites and check the visualization (<https://grafana.com/grafana/dashboards/>)



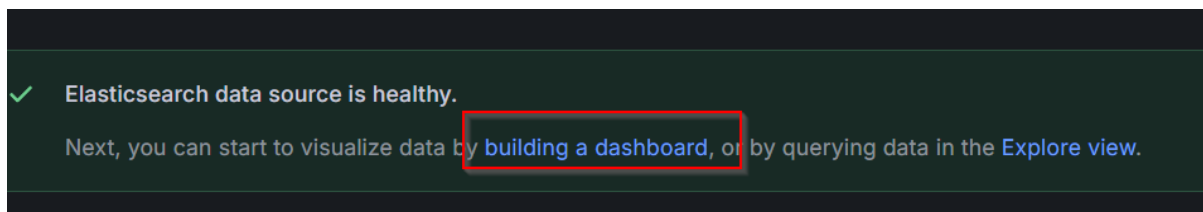


## Let's select the WAZUH SUMMARY DASHBAORD

(<https://grafana.com/grafana/dashboards/22448-wazuh-summary/>) and open it we can download json file or copy id










I have download Json format and next let's import the Json file and let's check visualization logs in dashboard and next check in data source is healthy pop-up there will be building a dashboard and click in and let's import wazuh summary Json format







EVENT ID 	AGENT 	IP ADDRESS 	RULE DESCRIPTION 	RULE LEVEL 
JF5QoJYBrm06OukJWyl1	Windows-server	192.168.31.214	Registry Key Entry Deleted.	5
1V5PoJYBrm06OukJ2IA1	Windows-server	192.168.31.214	Software protection service scheduled successfully.	3
IV5QoJYBrm06OukJWyl1	Windows-server	192.168.31.214	Registry Key Entry Deleted.	5
1F5PoJYBrm06OukJ2IA1	Windows-server	192.168.31.214	MISP - Error connecting to API	5
IF5QoJYBrm06OukJWyl1	Windows-server	192.168.31.214	Registry Key Entry Deleted.	5
0I5PoJYBrm06OukJnyCc	Windows-server	192.168.31.214	Sysmon - Event 22: DNS Request by C:\\Windows\\S	3
HF5QoJYBrm06OukJWyl1	Windows-server	192.168.31.214	Registry Key Entry Deleted.	5
0V5PoJYBrm06OukJmyC2	Windows-server	192.168.31.214	Sysmon - Event 22: DNS Request by C:\\Windows\\System32\\spoolsv.exe  	3
GI5QoJYBrm06OukJWyl1	Windows-server	192.168.31.214	Registry Key Entry Deleted.	5
2V5QoJYBrm06OukJGCC4	Windows-server	192.168.31.214	System time changed	5
KV5QoJYBrm06OukJWyl1	Windows-server	192.168.31.214	Registry Key Entry Deleted.	5
GF5QoJYBrm06OukJWyl1	Windows-server	192.168.31.214	Registry Key Entry Deleted.	5
KF5QoJYBrm06OukJWyl1	Windows-server	192.168.31.214	Registry Key Entry Deleted.	5
F15QoJYBrm06OukJWyl1	Windows-server	192.168.31.214	Registry Key Entry Deleted.	5