

Logging & Monitoring

What is Logging?

- Generates a detailed set of events that occur within your application
- Main purpose is to track error reporting and related data in a centralized way
- Logging frameworks:
 - Log4J (Java)
 - SLF4J (Java)
 - NLog (.NET)
 - Logging (Python)

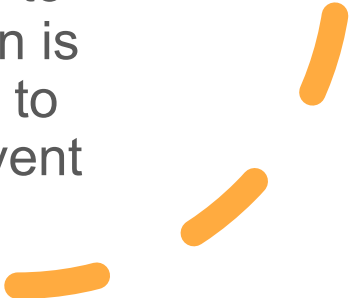


What is Monitoring?

- Technique of ensuring that an application both remains available and responds to user requests within an acceptable amount of time
- Instrumenting an application and then collecting, aggregating and analyzing metrics to improve your understanding of how the system behaves
- Monitoring toolkits:
 - **Prometheus**
 - Graphite
 - InfluxDB
 - OpenTSDB



Logging VS Monitoring?

- They serve two quite distinct purposes
 - Monitoring helps you manage application performance, while logging is all about managing the data inside logs
 - But they are very important for each other
 - Without properly managed logs that help find a cause of an application problem and make data available to application monitoring tools, you'll lack a critical source of data for monitoring
 - Without monitoring, you will not be able to make sense of log data in order to understand how your application is performing; nor will you be able to troubleshoot problems and prevent problems from recurring
- 



Prometheus

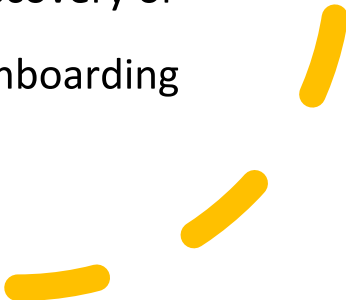
What is Prometheus?

- Prometheus is a leading open-source systems monitoring and alerting toolkit
- The software was created because of the need to monitor multiple microservices that might be running in your system
- Prometheus supports multiple exporters and helps getting started with specific monitoring requirements quickly.

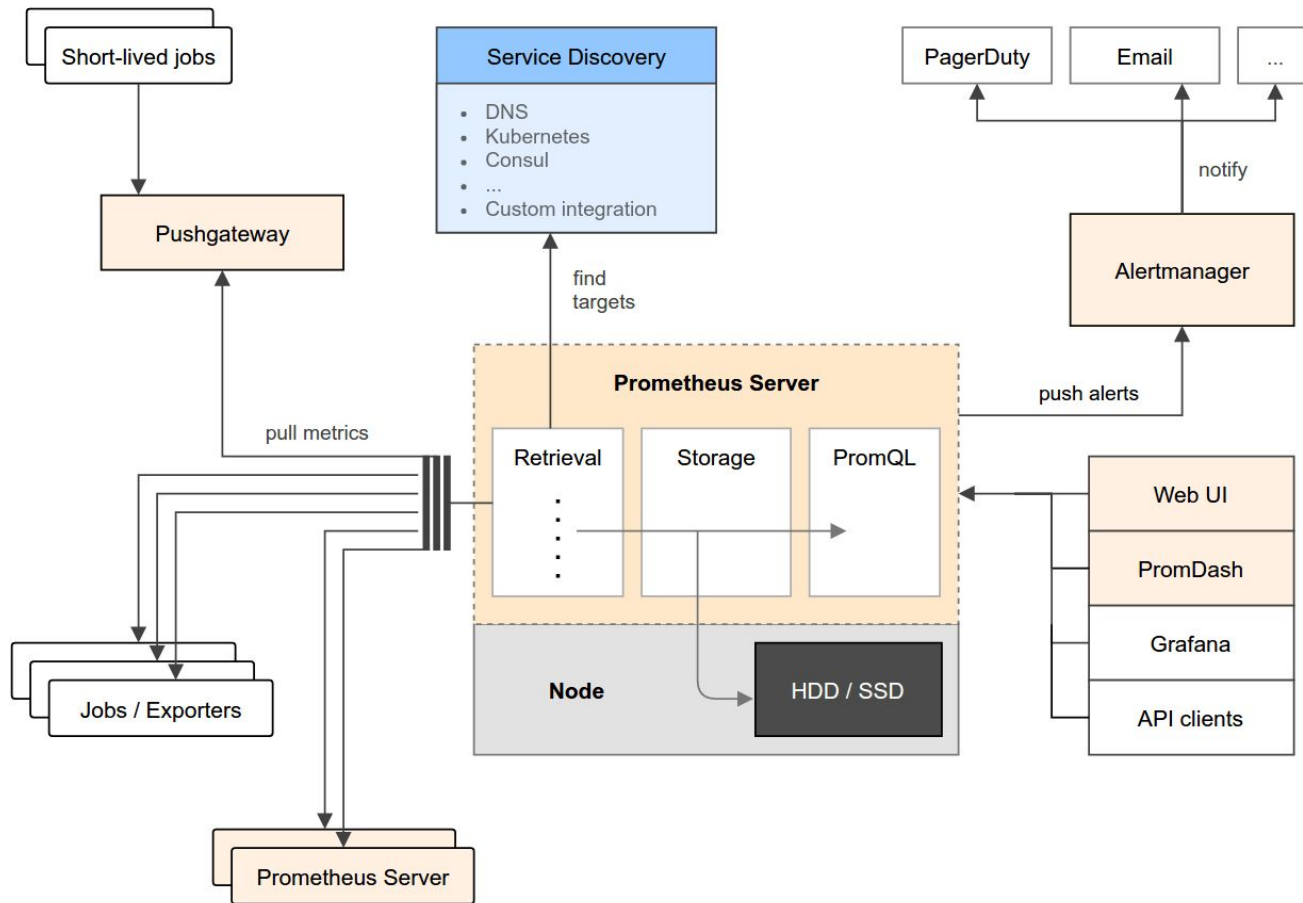


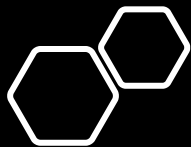
Features

- **Features**

- Prometheus's main features are:
 - a multi-dimensional data model with time series data identified by metric name and key/value pairs
 - PromQL, a flexible query language to leverage this dimensionality
 - no reliance on distributed storage; single server nodes are autonomous
 - time series collection happens via a pull model over HTTP
 - pushing time series is supported via an intermediary gateway
 - targets are discovered via service discovery or static configuration
 - multiple modes of graphing and dashboarding support
- 

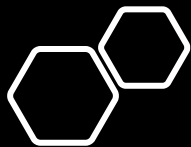
Prometheus Architecture





Components

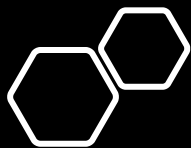
- The **Prometheus** ecosystem consists of multiple components, many of which are optional:
 - the main Prometheus server which scrapes and stores time series data
 - client libraries for instrumenting application code
 - a push gateway for supporting short-lived jobs
 - special-purpose exporters for services like HAProxy, StatsD, Graphite, etc.
 - an alertmanager to handle alerts
 - various support tools



Metric Types

The Prometheus client libraries offer four core metric types.

- Counter
- Gauge
- Histogram
- Summary



Visualization

- Expression Browser
- Grafana
- Console templates

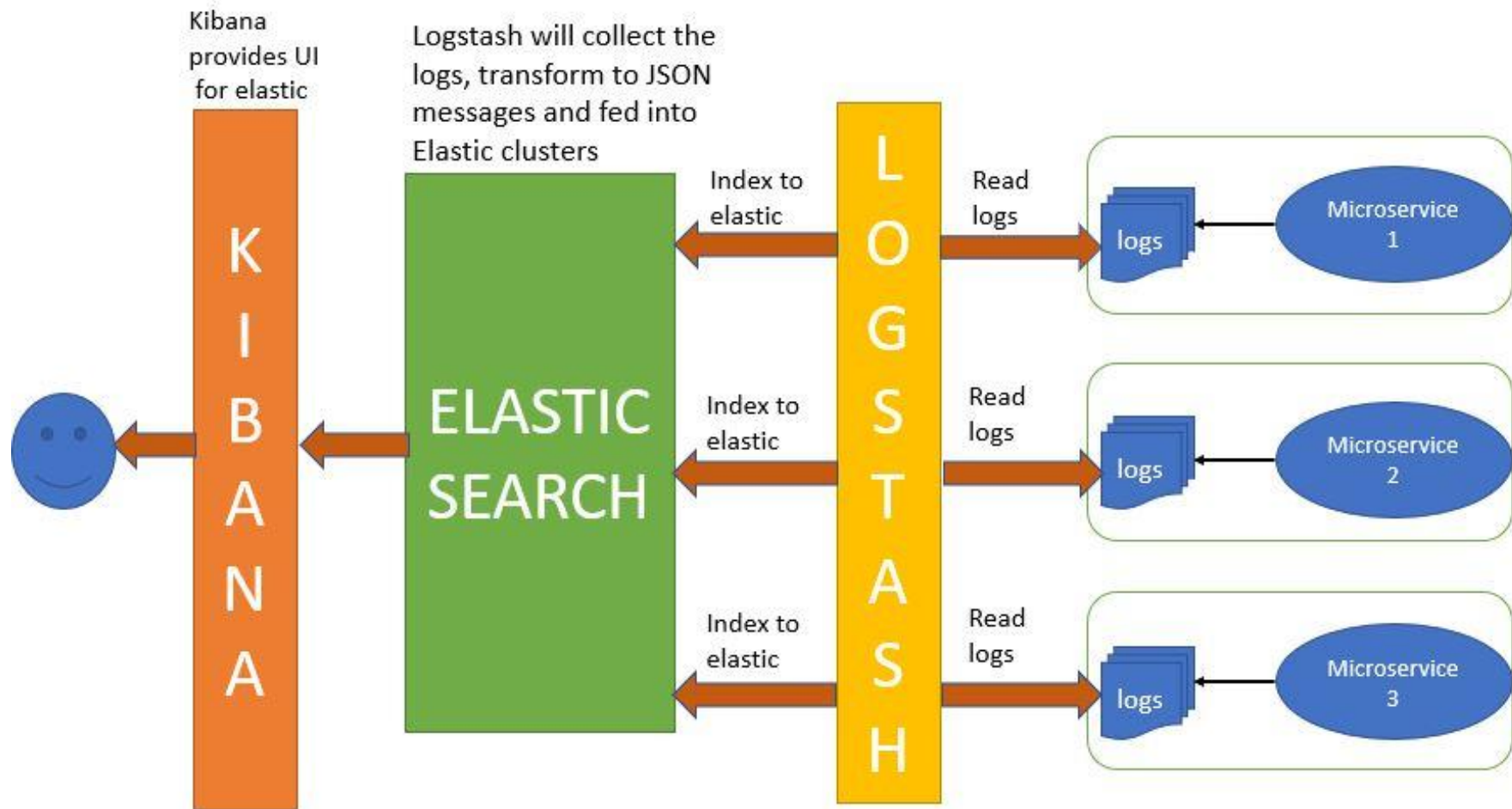
What is ELK Stack?

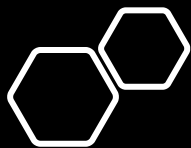


E - stands for **ElasticSearch**: used for storing logs

L - stands for **LogStash** : used for both shipping as well as processing and storing logs

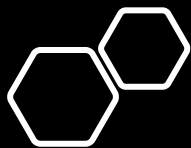
K - stands for **Kibana**: is a visualization tool (a web interface) which is hosted through Nginx or Apache





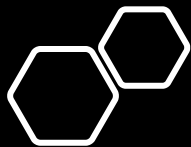
Elasticsearch

- Elasticsearch is a NoSQL database.
- It is based on Lucene search engine, and it is built with RESTful APIS.
- It offers simple deployment, maximum reliability, and easy management.



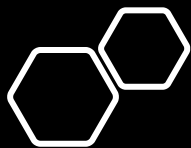
Elasticsearch Features

- Open source search server is written using Java
- Used to index any kind of heterogeneous data
- Has REST API web-interface with JSON output
- Full-Text Search
- Near Real Time (NRT) search
- Sharded, replicated searchable, JSON document store
- Schema-free, REST & JSON based distributed document store
- Multi-language & Geolocation support



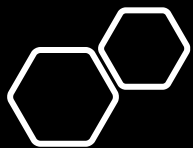
Elasticsearch Components

- Cluster (collection of nodes)
- Node (elasticsearch instance)
- Index (collection of documents)
- Document (basic unit of information)
- Shard (atomic part of index)



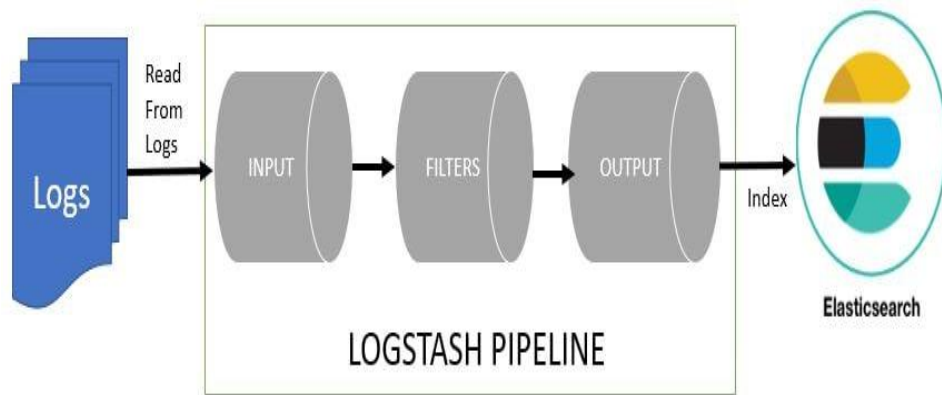
Logstash

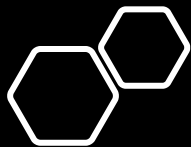
- Logstash is the data collection pipeline tool.
- It collects data inputs and feeds into the Elasticsearch.
- It gathers all types of data from the different source and makes it available for further use.



Logstash Components

- **Input:** passing logs to process them into machine understandable format
- **Filters:** It is a set of conditions to perform a particular action or event
- **Output:** Decision maker for processed event or log





Logstash Features

- Events are passed through each phase using internal queues
- Allows different inputs for your logs
- Filtering/parsing for your logs

Case studies

- Netflix
- LinkedIn
- Tripwire
- Medium





WHAT IS GRAFANA?

- **GRAFANA** is open source visualization and analytics software.
- It allows you to query, visualize, alert on and explore your metrics no matter where they are stored.
- It provides you with tools to turn your time-series database (TSDB) data into beautiful graphs and visualization.



PANELS

Graph Panel

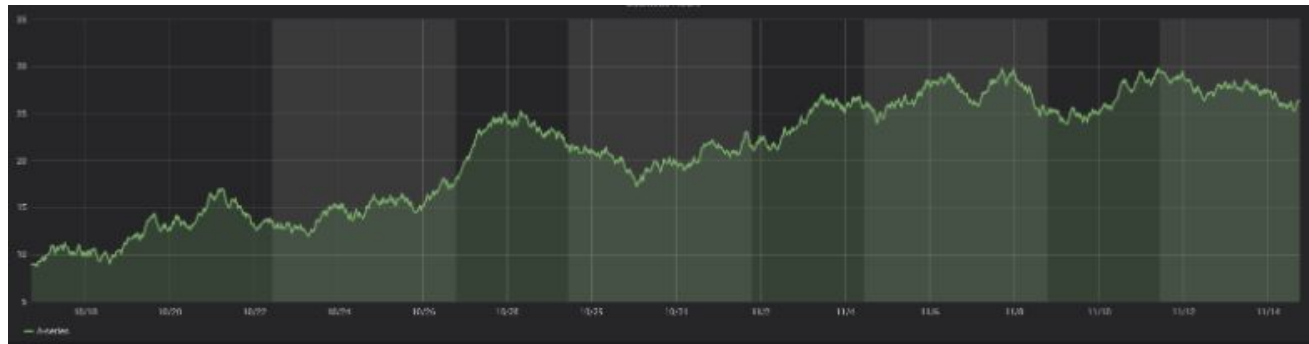


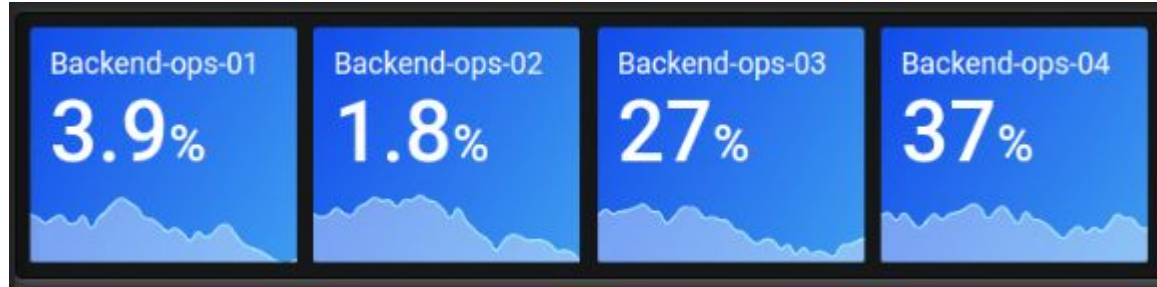
Table panel

Time series to columns				
Time ▾	backend_01	backend_02	backend_03	backend_04
2015-12-04 11:49:40	268 °F	273 °F	251 °F	250 °F
2015-12-04 11:49:20	267 °F	264 °F	283 °F	271 °F
2015-12-04 11:49:00	259 °F	267 °F	261 °F	266 °F
2015-12-04 11:48:40	295 °F	285 °F	294 °F	287 °F
2015-12-04 11:48:20	266 °F	281 °F	284 °F	282 °F
2015-12-04 11:48:00	279 °F	297 °F	295 °F	281 °F

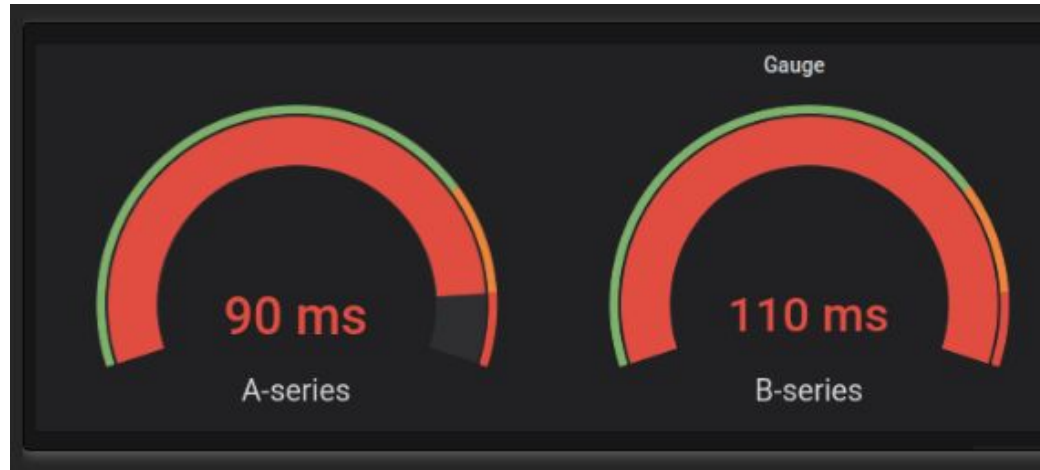
1 2 3 4 5 6 7 8 9

PANELS

Stat panel

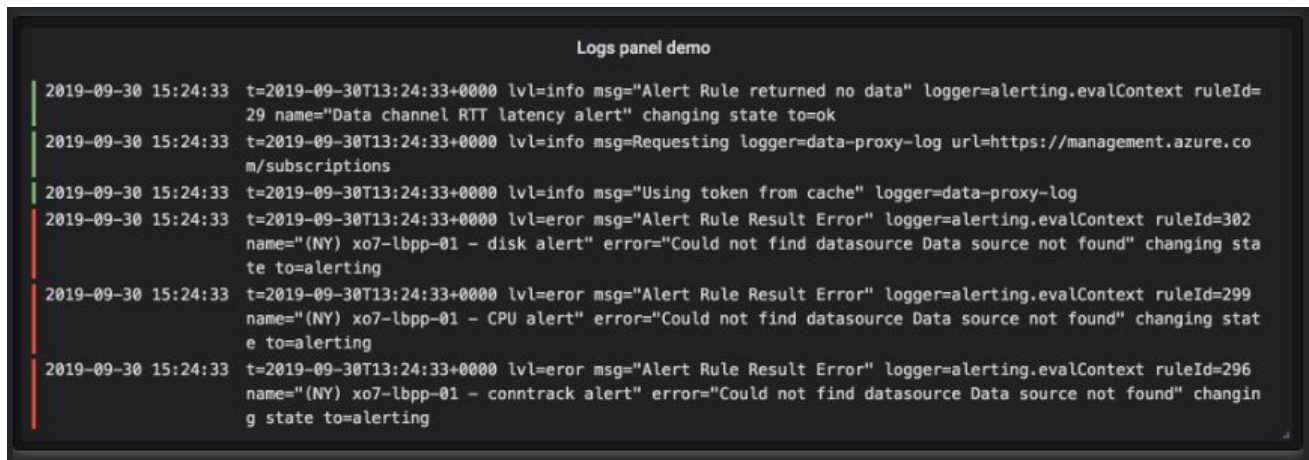


Gauge panel

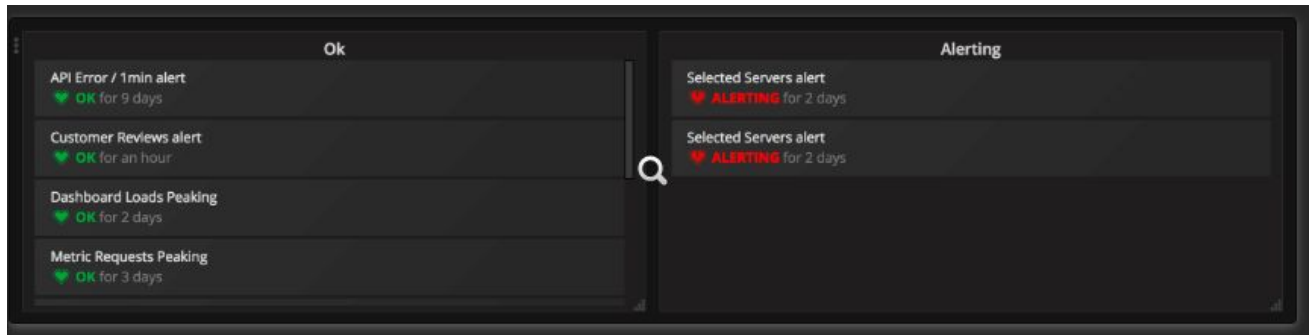


PANELS

Logs Panel



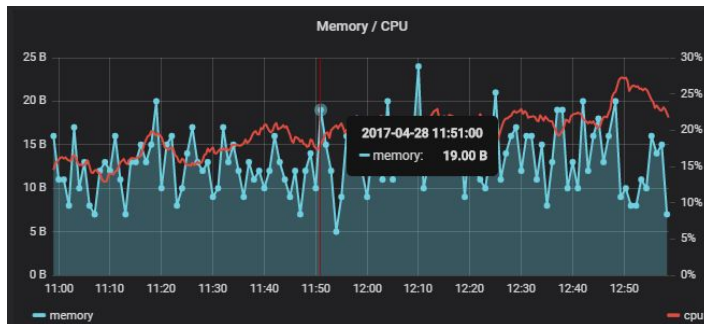
Alert List Panel



SHARE PANEL

- DIRECT LINK RENDERED IMAGE
 - You also get a link to render a PNG image of the panel. Useful if you want to share an image of the panel
- EMBED PANEL
 - You can embed a panel using an iframe on another web site.

```
<iframe src="https://snapshot.raintank.io/dashboard-solo/snapshot/y7zwi2bZ7FcoTlB93WN7yW04aMiz3pZb?from=1493369923321&to=1493377123321&panelId=4" width="650" height="300" frameborder="0"></iframe>
```



DATA SOURCES

Grafana ships with built in support for many Data Sources:

- AWS CloudWatch
- Azure Monitor
- **Elasticsearch**
- Google Stackdriver
- Graphite
- InfluxDB
- Microsoft SQL Server
- MySQL
- OpenTSDB
- PostgreSQL
- **Prometheus**

ALERTING

- Alerting in Grafana allows you to attach alerting rules to your dashboard panels.
- In the alert tab of the graph panel you can configure how often the alert rule should be evaluated and the conditions that need to be met for the alert to change state and trigger its notifications

The screenshot shows the Grafana Alerting configuration interface for a 'Graph' panel. The 'Alert' tab is selected and highlighted with a red box. The 'Alert Config' section shows the alert name 'Site Logins Too Low' and the evaluation frequency 'Evaluate every 10s', both highlighted with red boxes. The 'Conditions' section is also highlighted with a red box and contains a single condition: 'WHEN avg () OF query (A, 5m, now) IS BELOW 45'. Below the conditions, there is a '+ ' button to add more conditions. At the bottom, the 'SET STATE TO' dropdown is set to 'No Data'.

Graph General Metrics Axes Legend Display **Alert** Time range

Alert Config

Name Site Logins Too Low Evaluate every 10s

Conditions

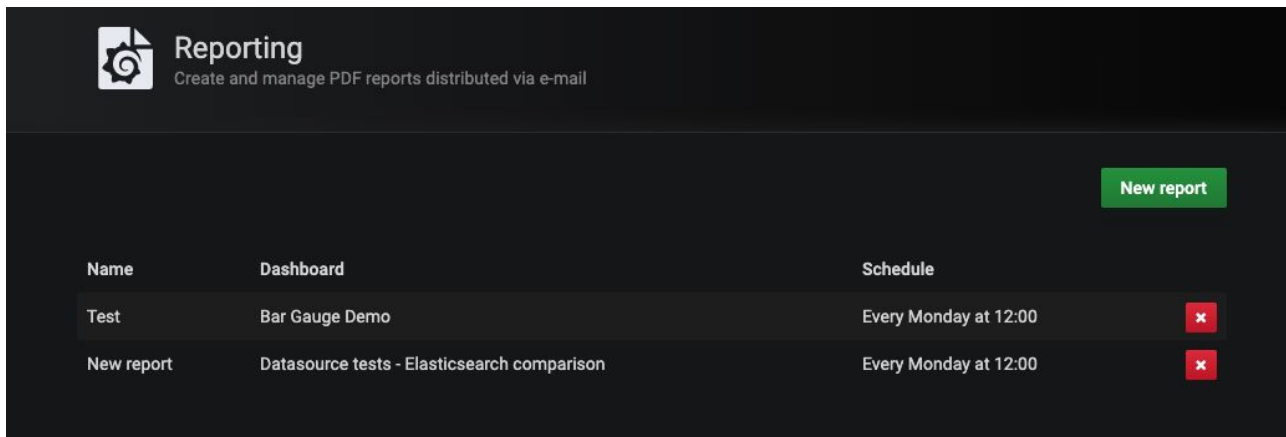
WHEN avg () OF query (A, 5m, now) IS BELOW 45

+

If no data points or all values are null SET STATE TO No Data

REPORTING

- Reporting allows you to generate PDFs from any of your dashboards and have them sent out to interested parties on a schedule.



- ... and a lot of other Grafana interesting and useful features that can be found in the official docs:
<https://grafana.com/docs/grafana/latest/>



What is Kibana?

- It is a visualization tool like Grafana
- Pros:
 - Easier to set up
 - If you are using ELK stack
 - Log analysis: supports querying on text data
- Cons:
 - Supports integration only with Elasticsearch
 - Not so rich visualization features
 - Does not offer support for Alerts out of the box. Requires 3rd party integration to enable Alerts

