



Observability

DIEGO PACHECO



Stack

About me...



- Cat's Father
- Principal Software Architect
- Agile Coach
- SOA/Microservices Expert
- DevOps Practitioner
- Speaker
- Author

 diegopacheco

 @diego_pacheco

 <http://diego-pacheco.blogspot.com.br/>



<https://diegopacheco.github.io/>

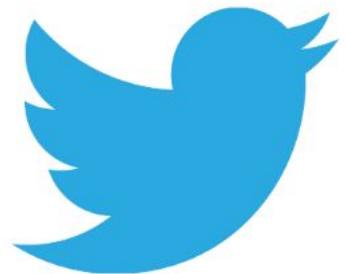
Observability

Observability

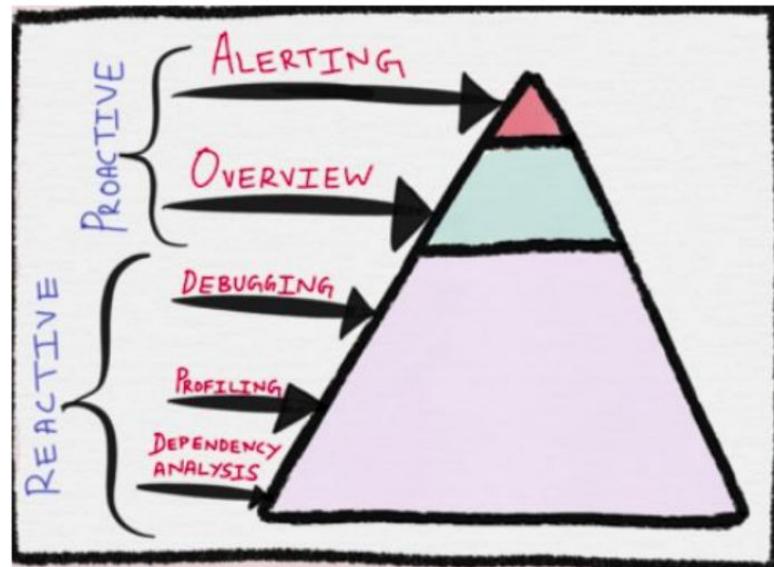
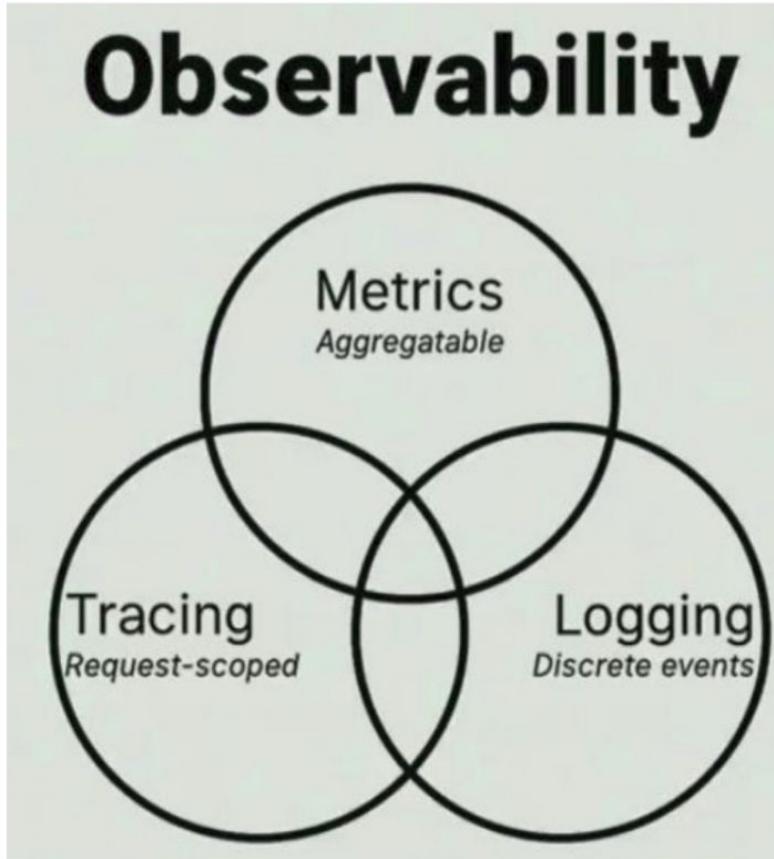
From Wikipedia, the free encyclopedia

For the concept in quantum mechanics, see [observable](#).

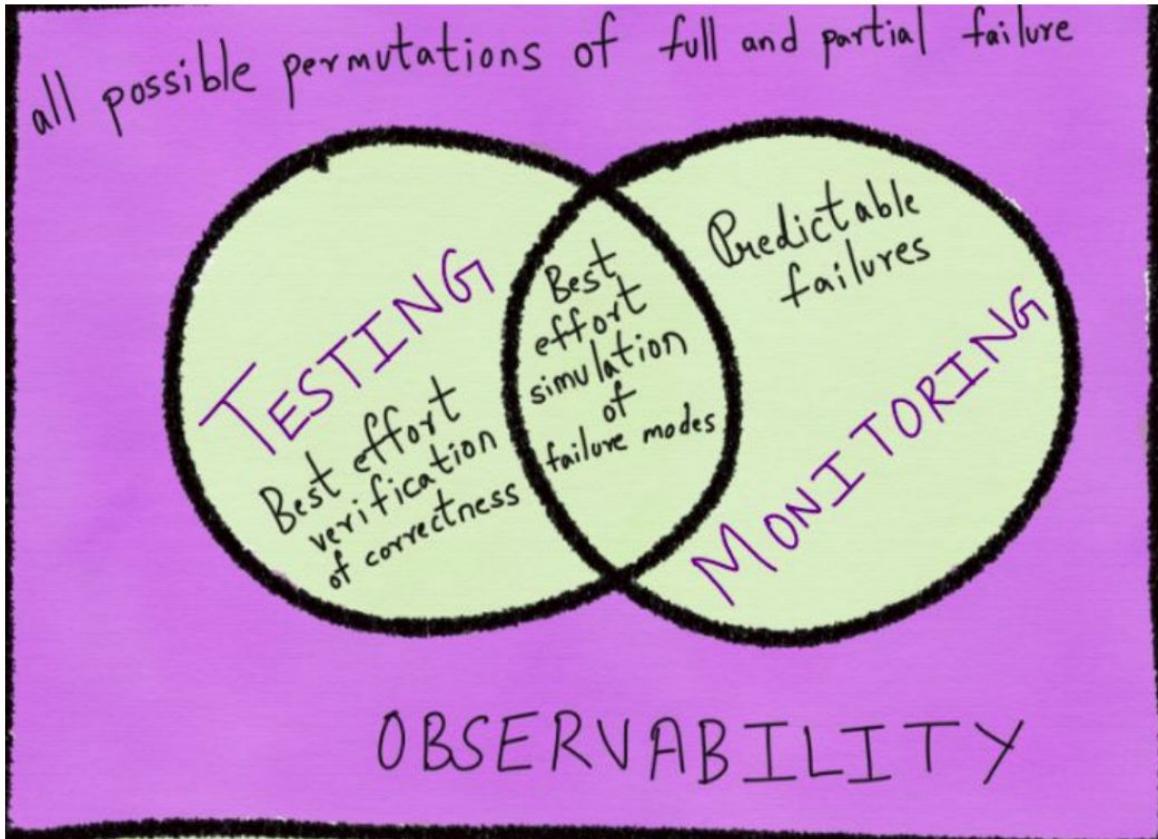
In control theory, **observability** is a measure of how well internal states of a [system](#) can be inferred from knowledge of its external outputs. The observability and [controllability](#) of a system are mathematical [duals](#). The concept of observability was introduced by Hungarian-American engineer Rudolf E. Kálmán for linear dynamic systems.^{[1][2]}



Observability

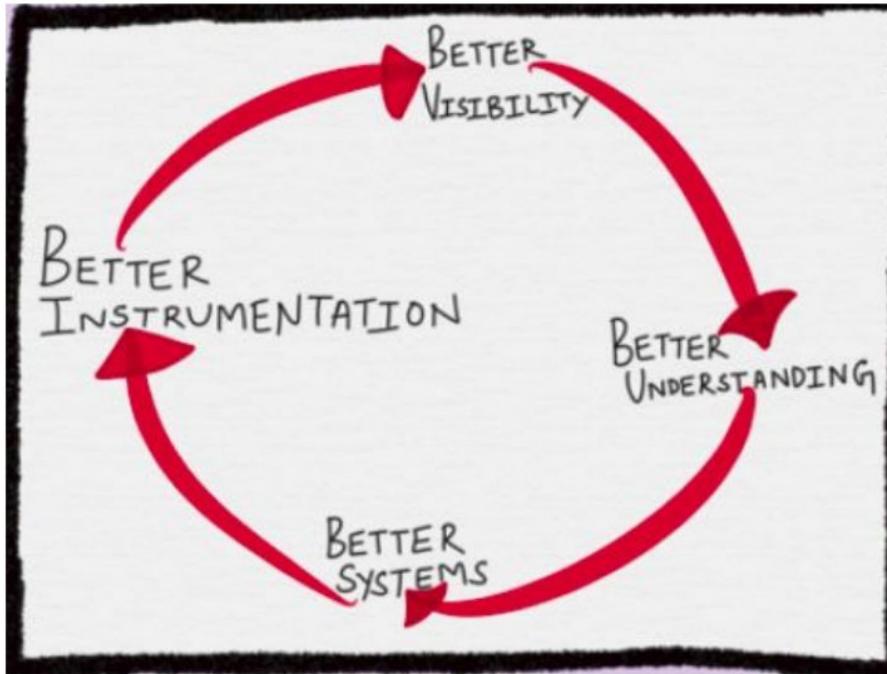


Observability



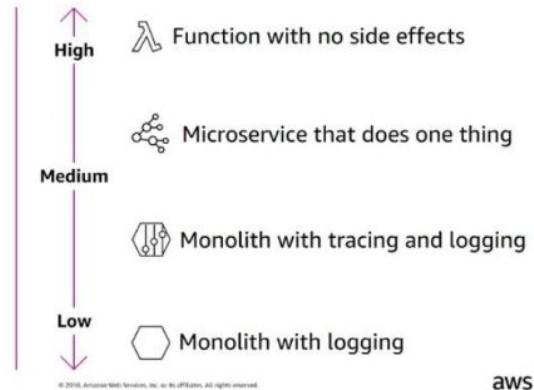
Observability

Observability Cycle



Observability

re:Invent



© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Observability

Alerts for Alerts are WRONG!

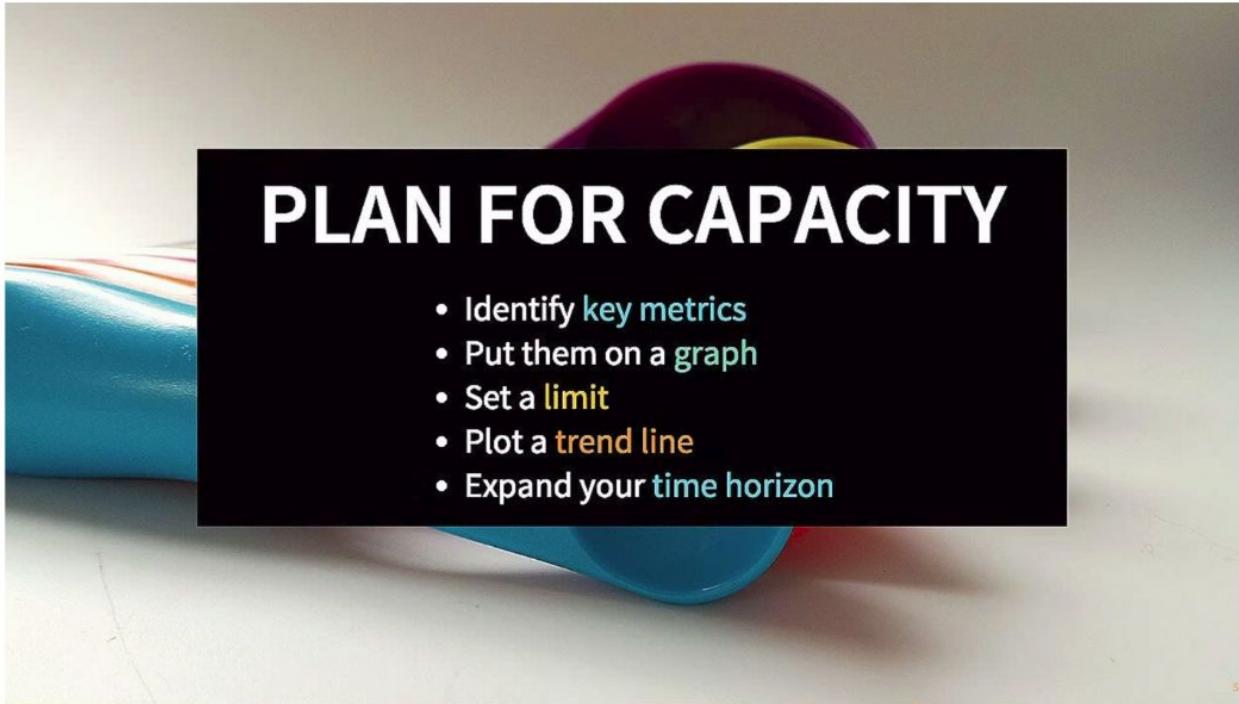


**ONLY ALERT ON WHAT
IS ACTIONABLE**

- Get the attention of the **right** humans
- As **few alerts** as possible
- Routed to the people who can take action

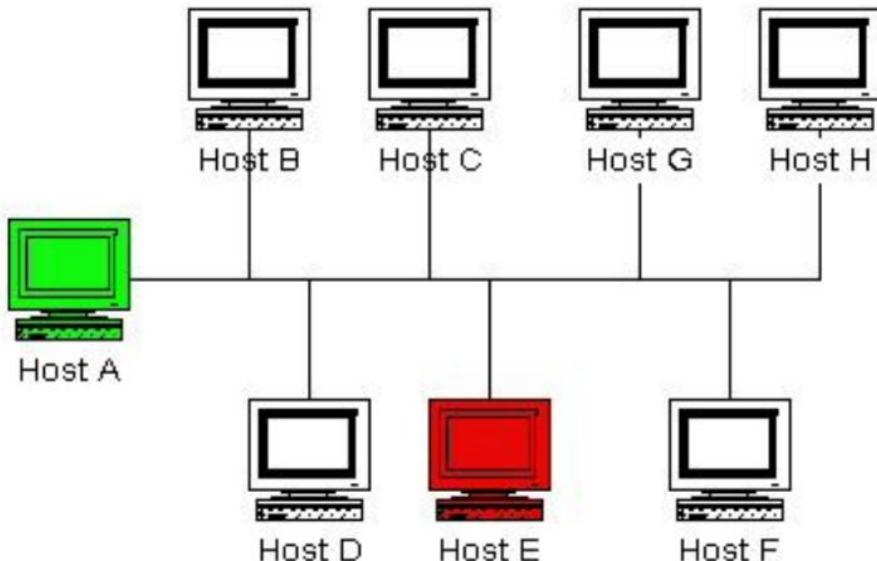
Observability

Capacity Planning



Observability

Host Monitoring



ZABBIX

Observability

Remember the Cloud...

Pets

vs

Cattle



Unique and
Indispensable

GUI Driven
Ticket Based
Hand Crafted
Reserved
Scale-Up
Smart Hardware
Proprietary
“Waterfall Ops”



Disposable,
One of the
Herd

API Driven
Self Service
Automated
On Demand
Scale-Out
Smart Apps
Open Source
Agile DevOps

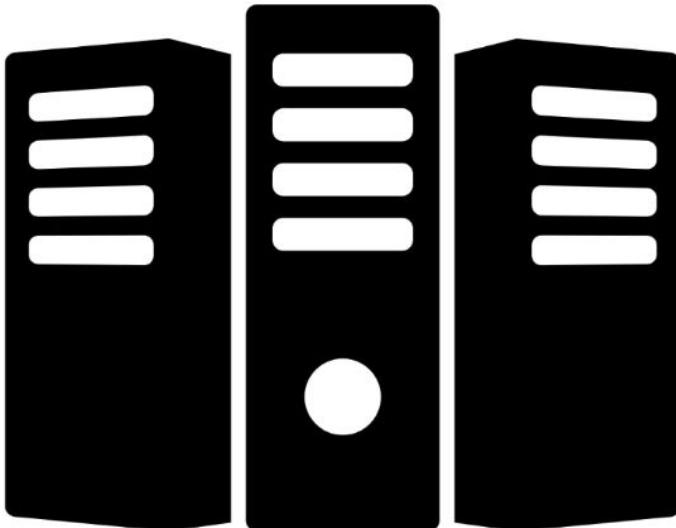
Observability

Time Series Databases



Observability

Application Expose Metrics



- Black box monitoring dont work any more
- Health/Ping/UP Status are not enough
- Need to send All kinds of metrics like:
 - OS(CPU, Memory, Disk, Network)
 - App(Latency, Requests, Custom)
 - Biz (Transactions, Purchases, etc..)
- This metrics cannot be processed in place
- They need to goto a time series database
- Where we can do Aggregation and Signal Processing and CO RELATE events.

Observability

Expose what?

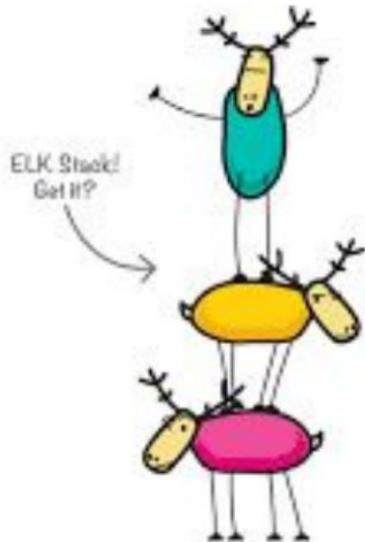
What Kinds Of Telemetry Should You Emit?

<u>Popular Systems/Methods/Blueprints</u>	<u>Formal Laws of Performance</u>
USE Method <ul style="list-style-type: none">• Utilization, Saturation, Errors	Queueing Theory <ul style="list-style-type: none">• Utilization, arrival rate, throughput, latency
RED Method <ul style="list-style-type: none">• Requests, Errors, Duration	Little's Law <ul style="list-style-type: none">• Concurrency, latency, throughput
SRE Book's Four Golden Signals <ul style="list-style-type: none">• Latency, traffic, errors, and saturation	Universal Scalability Law <ul style="list-style-type: none">• Throughput, concurrency

@scprb

Observability

ELK



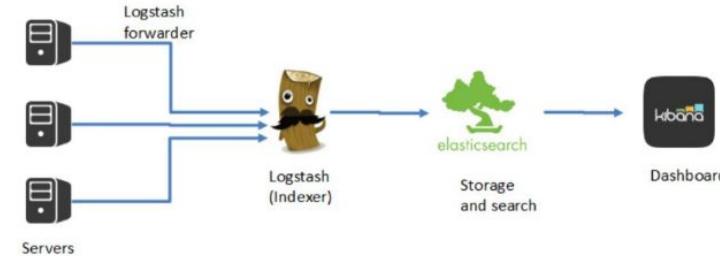
E Elasticsearch

L Logstash

K Kibana



ELK Architecture



Observability

Grafana



Observability

Prometheus



Prometheus

⚠ Dimensional data

Prometheus implements a highly dimensional data model. Time series are identified by a metric name and a set of key-value pairs.

🔍 Powerful queries

PromQL allows slicing and dicing of collected time series data in order to generate ad-hoc graphs, tables, and alerts.

📈 Great visualization

Prometheus has multiple modes for visualizing data: a built-in expression browser, Grafana integration, and a console template language.

📀 Efficient storage

Prometheus stores time series in memory and on local disk in an efficient custom format. Scaling is achieved by functional sharding and federation.

⚙ Simple operation

Each server is independent for reliability, relying only on local storage. Written in Go, all binaries are statically linked and easy to deploy.

⚠ Precise alerting

Alerts are defined based on Prometheus's flexible PromQL and maintain dimensional information. An alertmanager handles notifications and silencing.

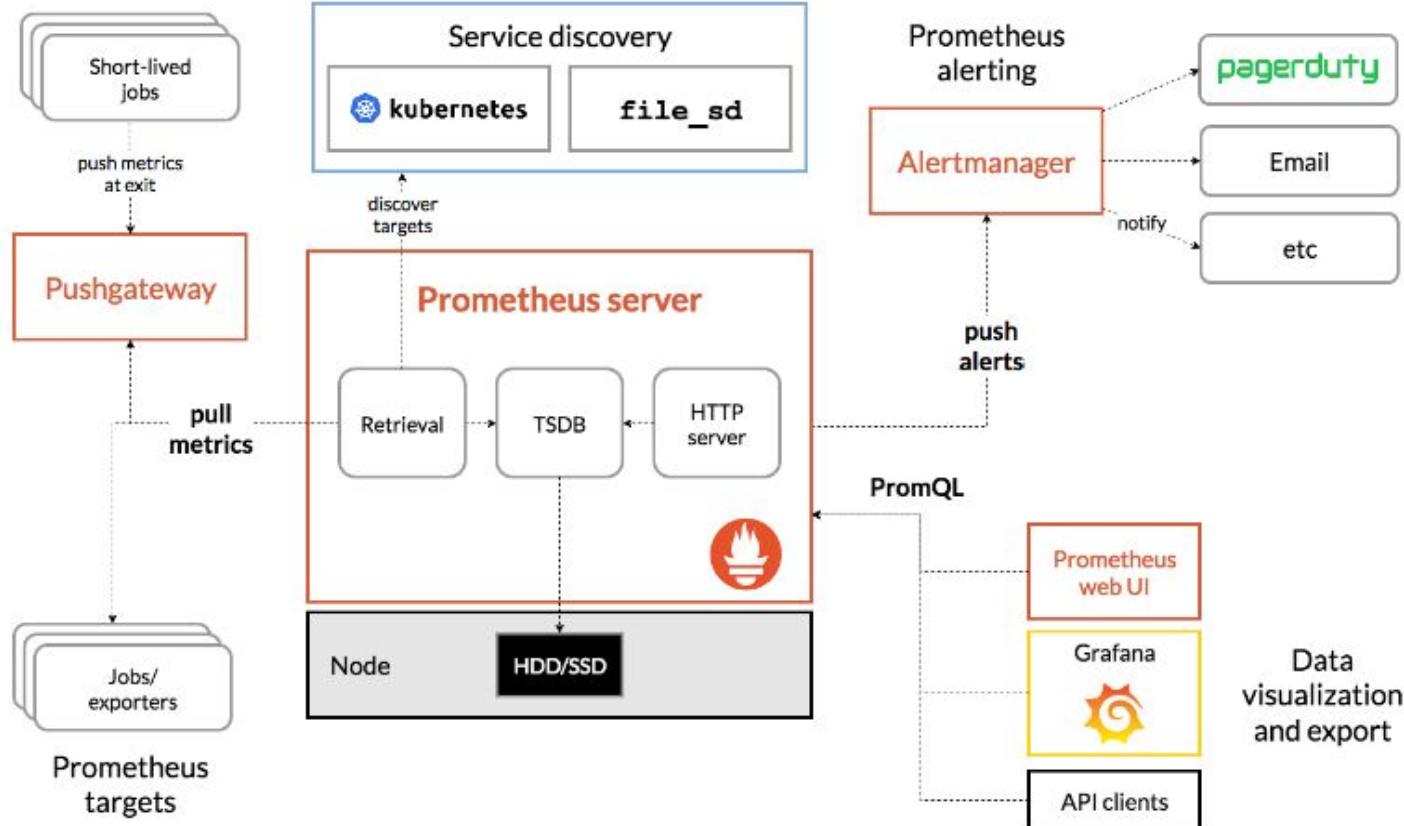
</> Many client libraries

Client libraries allow easy instrumentation of services. Over ten languages are supported already and custom libraries are easy to implement.

☁ Many integrations

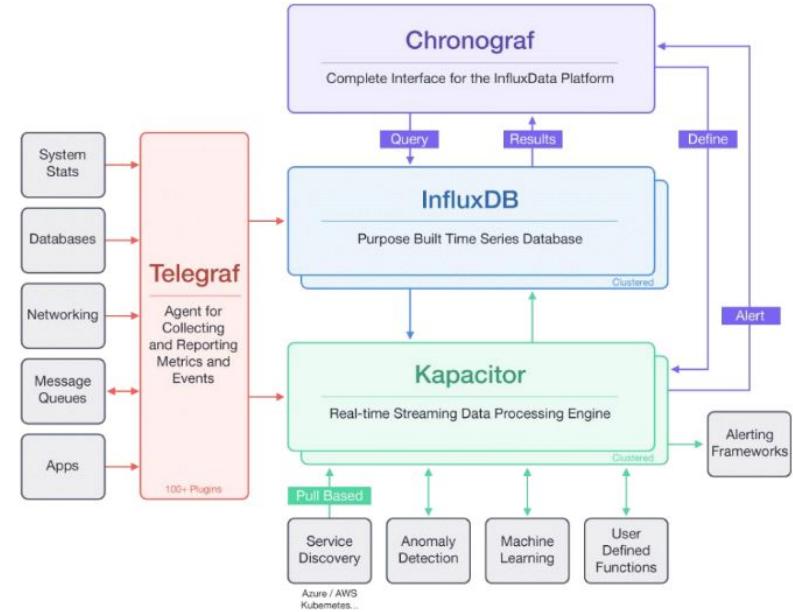
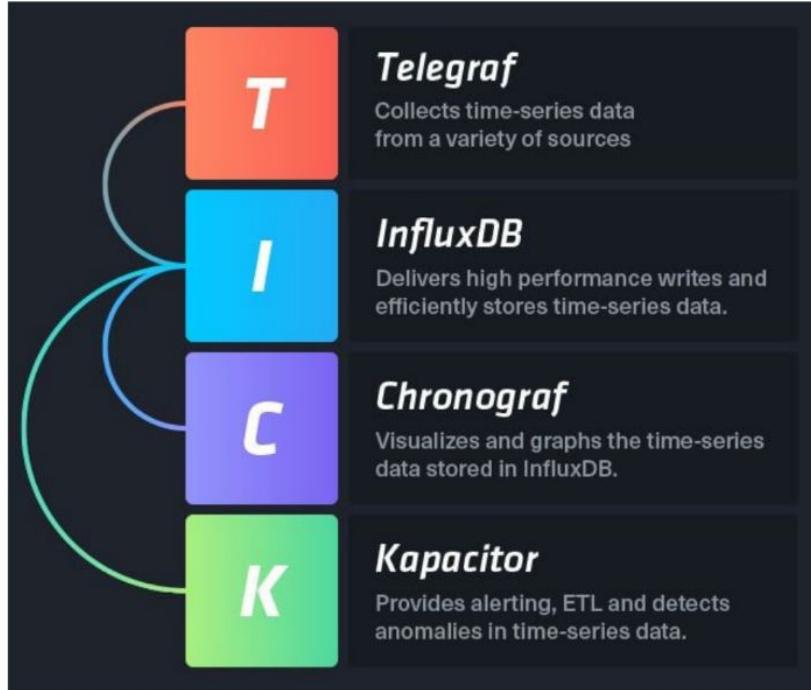
Existing exporters allow bridging of third-party data into Prometheus. Examples: system statistics, as well as Docker, HAProxy, StatsD, and JMX metrics.

Observability - Prometheus Architecture



Observability

Influx - TICK



Observability

CollectD



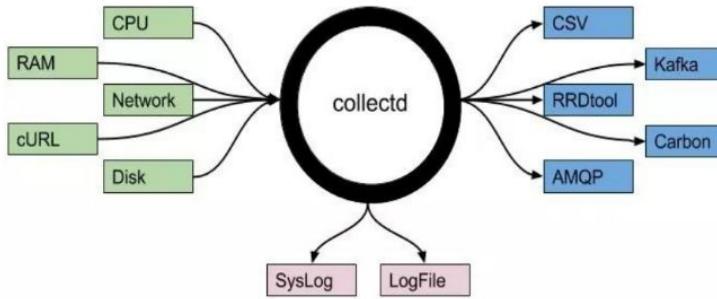
```
Hostname      "test.example.com"
LoadPlugin interface
LoadPlugin load
LoadPlugin memory
LoadPlugin network
LoadPlugin logfile

<Plugin logfile>
    LogLevel info
    File "/var/log/collectd.log"
</Plugin>
<Plugin interface>
    Interface "eth0"
    IgnoreSelected false
</Plugin>
<Plugin network>
    Server "172.20.1.10" "7070"
</Plugin>
```

```
Logstash Config :

input {
  udp {
    port => 7070
    buffer_size => 1452
    codec => collectd { }
    type => "collectd"
  }
}
output {
  stdout { codec => json }
}
```

- ❑ OLD
- ❑ Everybody use it
- ❑ Lots of Plugins and plug and play metrics
- ❑ HARD TO TEST
- ❑ HARD TO TROUBLESHOOT
- ❑ Need to RESET in order to change configs(FS)



Observability

Centralized Logging



Observability

Graylog 2

graylog

The screenshot shows the Graylog 2 web interface with the following details:

- Header:** Shows the Graylog 2 logo and navigation links: messages, streams, analytics, hosts, blacklists, settings.
- Left Sidebar:** Displays a list of log entries under the 'Messages' section. The first few entries are:
 - 2012-10-20 08:27:05.564 info system daemontest user="laurens" auto-pastethear name="Padam accepted" action="accept"
 - 2012-10-20 08:27:05.579 info pfSense.achitz.org local0 pf 00:00:00:00:00:00 wlan0[match] pass in on em1: (loc 0x0, id 44, offset 0, flags [DF], proto TCP (1), length 60)
 - 2012-10-20 08:27:05.579 info pfSense.achitz.org local0 pf 192.168.0.1:63.51.63.792 > 192.168.0.12.1248: Flags [S], cksum 0x7d3f (correct), seq 47620459, win 5840, options [mss 1460,sackOK,T5 val 38337]
- Right Sidebar:** Shows a 'Welcome, admin!' message, current time (30.10.2012 - 07:37:08), and a line chart titled 'Welcome, admin!'. The chart shows a single pink line starting at 0, peaking around 3500 at 0:30, and ending at approximately 2500 at 0:36.
 - Jobs & Tasks: Shows 0 broken subscriptions, 0 not running, and 0 stream alerts.
 - Open dashboard: A button to open the dashboard.
 - Server health: A link to check server health.

Observability

ELK

Kibana

Discover Visualize Dashboard Settings

Last 15 minutes

[filebeat-YYYY.MM.DD]

Selected Fields: _source

Available Fields: @timestamp, @version, _id, _index, _score, _type, beat.hostname, beat.name, count, fields, host, input_type, message, offset, source

Count: January 29th 2016, 15:27:05.719 - January 29th 2016, 15:42:05.719 — by 30 seconds

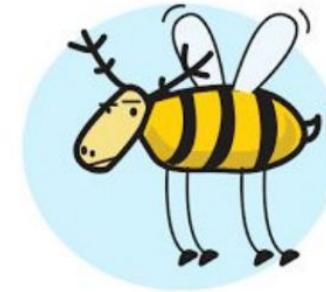
42 hits

Time: January 29th 2016, 15:41:52.713

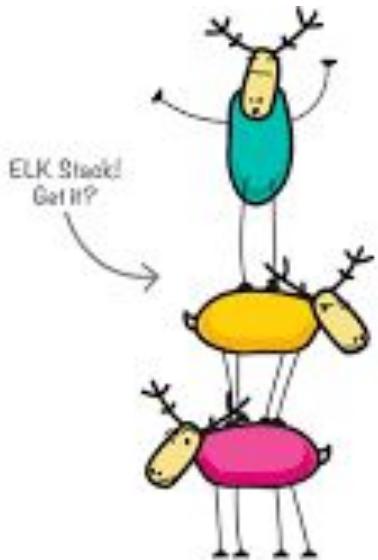
_source: message: Jan 29 15:41:47 topbeat-u-03 sshd[4913]: Invalid user tomcat from 202.70.78.254 @version: 1 @timestamp: January 29th 2016, 15:41:52.713 beat.hostname: topbeat-u-03 beat.name: topbeat-u-03 count: 1 fields: - input_type: log offset: 1,419,122 source: /var/log/auth.log type: log host: topbeat-u-03 _id: AVKPHvg6ahvshQLa56a7 _type: log _index: filebeat-2016.01.29 _score: -

Time: January 29th 2016, 15:41:52.713

_source: message: Jan 29 15:41:47 topbeat-u-03 sshd[4913]: pam_unix(sshd:auth): check pass; user unknown @version: 1 @timestamp: January 29th 2016, 15:41:52.713 beat.hostname: topbeat-u-03 beat.name: topbeat-u-03 count: 1 fields: - input_type: log offset: 1,419,297 source: /var/log/auth.log type: log host: topbeat-u-03 _id: AVKPHvg6ahvshQLa56a9 _type: log _index: filebeat-2016.01.29 _score: -



ELK

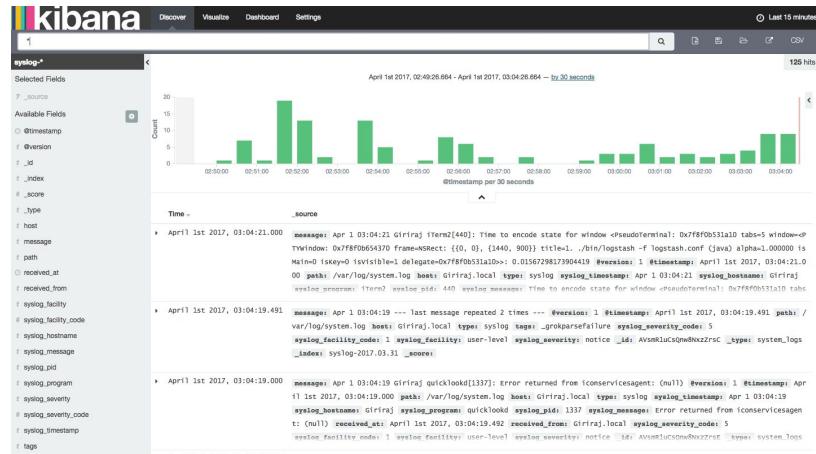


E Elasticsearch

L Logstash

K Kibana

<https://www.elastic.co/what-is/elk-stack>



<https://elk-docker.readthedocs.io/>

ELK

```
sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name elk sebp/el

File Edit View Search Terminal Tabs Help
sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name elk sebp/el
diego@4winds: ~
diego@4winds: ~/github/diegopacheco/linux/scripts

sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name elk sebp/el

diego@4winds: ~
diego@4winds: ~/github/diegopacheco/linux/scripts

libs/icon.app_spaces-js.bundle.dll.js", "method": "get", "headers": {"host": "localhost:5601", "connection": "keep-alive", "user-agent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36", "accept": "*/*", "sec-fetch-site": "same-origin", "sec-fetch-mode": "no-cors", "referer": "http://localhost:5601/app/kibana", "accept-encoding": "gzip, deflate, br", "accept-language": "en-US,en;q=0.9,pt-BR;q=0.8,pt;q=0.7,es;q=0.6", "if-none-match": "\\"940755afb6ac9d0b1a3cd74b4379d59c73e098ad-/built_assets/dlls/-gziip\\\"", "remoteAddress": "172.17.0.1", "userAgent": "172.17.0.1", "referer": "http://localhost:5601/app/kibana"}, "res": {"statusCode": 304, "responseTime": 18, "contentLength": 9}, "message": "GET /built_assets/dlls/icon.app_spaces-js.bundle.dll.js 304 18ms - 9.0B" }
{"type": "response", "@timestamp": "2019-12-13T10:34:09Z", "tags": [], "pid": 325, "method": "get", "statusCode": 304, "req": {"url": "/built_assets/dlls/icon.app_watches-js.bundle.dll.js", "method": "get", "headers": {"host": "localhost:5601", "connection": "keep-alive", "user-agent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36", "accept": "*/*", "sec-fetch-site": "same-origin", "sec-fetch-mode": "no-cors", "referer": "http://localhost:5601/app/kibana", "accept-encoding": "gzip, deflate, br", "accept-language": "en-US,en;q=0.9,pt-BR;q=0.8,pt;q=0.7,es;q=0.6", "if-none-match": "\\"c4f4504d7fa825bd9a7f3495ba1a0e43aab7594-/built_assets/dlls/-gziip\\\"", "remoteAddress": "172.17.0.1", "userAgent": "172.17.0.1", "referer": "http://localhost:5601/app/kibana"}, "res": {"statusCode": 304, "responseTime": 7, "contentLength": 9}, "message": "GET /built_assets/dlls/icon.app_watches-js.bundle.dll.js 304 7ms - 9.0B" }
{"type": "response", "@timestamp": "2019-12-13T10:34:09Z", "tags": [], "pid": 325, "method": "get", "statusCode": 304, "req": {"url": "/ui/fonts/intel-ui/Inter-UI-Light-BETA.woff2", "method": "get", "headers": {"host": "localhost:5601", "connection": "keep-alive", "origin": "http://localhost:5601", "user-agent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36", "accept": "*/*", "sec-fetch-site": "same-origin", "sec-fetch-mode": "cors", "referer": "http://localhost:5601/app/kibana", "accept-encoding": "gzip, deflate, br", "accept-language": "en-US,en;q=0.9,pt-BR;q=0.8,pt;q=0.7,es;q=0.6", "if-none-match": "\\"15e14698571lbc9631d87ffa1df8bcd2036ef3\\\"", "if-modified-since": "Fri, 27 Sep 2019 09:10:54 GMT", "remoteAddress": "172.17.0.1", "userAgent": "172.17.0.1", "referer": "http://localhost:5601/app/kibana"}, "res": {"statusCode": 304, "responseTime": 3, "contentLength": 9}, "message": "GET /ui/fonts/inter_ui/Inter-UI-Light-BETA.woff2 304 3ms - 9.0B" }
{"type": "response", "@timestamp": "2019-12-13T10:34:09Z", "tags": [], "pid": 325, "method": "get", "statusCode": 304, "req": {"url": "/ui/fonts/intel-ui/Inter-UI-Bold.woff2", "method": "get", "headers": {"host": "localhost:5601", "connection": "keep-alive", "origin": "http://localhost:5601", "user-agent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36", "accept": "*/*", "sec-fetch-site": "same-origin", "sec-fetch-mode": "cors", "referer": "http://localhost:5601/app/kibana", "accept-encoding": "gzip, deflate, br", "accept-language": "en-US,en;q=0.9,pt-BR;q=0.8,pt;q=0.7,es;q=0.6", "if-none-match": "\\"ef58983e63f29692b7cea49c314e57bc63de763f\\\"", "if-modified-since": "Fri, 27 Sep 2019 09:10:54 GMT", "remoteAddress": "172.17.0.1", "userAgent": "172.17.0.1", "referer": "http://localhost:5601/app/kibana"}, "res": {"statusCode": 304, "responseTime": 2, "contentLength": 9}, "message": "GET /ui/fonts/inter_ui/Inter-UI-Bold.woff2 304 2ms - 9.0B" }
```

ELK

Kibana x +

localhost:5601/app/kibana#/home?_g=()

D Home

Add Data to Kibana

Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems.

 APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

[Add APM](#)

 Logging

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

[Add log data](#)

 Metrics

Collect metrics from the operating system and services running on your servers.

[Add metric data](#)

 SIEM

Centralize security events for interactive investigation in ready-to-go visualizations.

[Add security events](#)

Add sample data
Load a data set and a Kibana dashboard

Upload data from log file
Import a CSV, NDJSON, or log file

Use Elasticsearch data
Connect to your Elasticsearch index

Visualize and Explore Data

Manage and Administer the Elastic Stack



ELK



The screenshot shows a web browser window with the URL `localhost:9200`. The page displays the Elasticsearch configuration object, which includes details like the cluster name, UUID, and various version numbers. The code is color-coded for readability.

```
// 20191213073339
// http://localhost:9200/
{
  "name": "elk",
  "cluster_name": "elasticsearch",
  "cluster_uuid": "vNj_F2ljSXeuFTiR017pkQ",
  "version": {
    "number": "7.4.0",
    "build_flavor": "default",
    "build_type": "tar",
    "build_hash": "22e1767283e61a198cb4db791ea66e3f11ab9910",
    "build_date": "2019-09-27T08:36:48.569419Z",
    "build_snapshot": false,
    "lucene_version": "8.2.0",
    "minimum_wire_compatibility_version": "6.8.0",
    "minimum_index_compatibility_version": "6.0.0-beta1"
  },
  "tagline": "You Know, for Search"
}
```

ELK: Create a document and query

Create Document

```
curl -H 'Content-Type: application/json' -XPUT 'localhost:9200/customer/_create/1' -d '  
{  
  "name": "John Doe 1"  
}'
```

Search

```
curl --silent -X GET "http://localhost:9200/customer/_search?q=*" | jq .
```

ELK: Query ES

```
diego@4winds: ~/github/diegopacheco/linux/scripts
File Edit View Search Terminal Tabs Help
diego@4winds: ~/github/diegopacheco/linux/scripts      x  sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name elk sebp/elk  x  07:51:20  6.56G  1.71
diego@4winds: ~/github/diegopacheco/linux/scripts  ↵ master  ↵ master  curl --silent -X GET "http://localhost:9200/customer/_search?q=*" | jq .
{
  "took": 1,
  "timed_out": false,
  "_shards": {
    "total": 1,
    "successful": 1,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 1,
      "relation": "eq"
    },
    "max_score": 1,
    "hits": [
      {
        "_index": "customer",
        "_type": "_doc",
        "_id": "1",
        "_score": 1,
        "_source": {
          "name": "John Doe 1"
        }
      }
    ]
  }
}
diego@4winds: ~/github/diegopacheco/linux/scripts  ↵ master  ↵  07:52:33  6.62G  1.76
```

ELK: Setup Index and add documents

```
diego@4winds ~ - curl -H 'Content-Type: application/json' -XPUT 'localhost:9200/customer'  
{"acknowledged":true,"shards_acknowledged":true,"index":"customer"}  
diego@4winds ~ - curl -H 'Content-Type: application/json' -XPUT 'localhost:9200/customer/_create/1' -d '  
{  
  "name": "John Doe 1"  
}  
{"_index":"customer","_type":"_doc","_id":"1","_version":1,"result":"created","_shards":{"total":2,"successful":1,"failed":0},"_seq_no":0,"_primary_term":1}  
diego@4winds ~ - curl -H 'Content-Type: application/json' -XPUT 'localhost:9200/customer/_create/2' -d '  
{  
  "name": "John Doe 2"  
}  
{"_index":"customer","_type":"_doc","_id":"2","_version":1,"result":"created","_shards":{"total":2,"successful":1,"failed":0},"_seq_no":1}
```

ELK: Setup Index Pattern in Kibana and them query

The screenshot shows the Kibana Discover interface. At the top, there are tabs for 'Discover' (selected), 'Dashboard', and 'Visualize'. Below the tabs is a navigation bar with icons for 'New', 'Save', 'Open', 'Share', and 'Inspect'. A search bar contains the text '# < Search' and a 'KQL' button. To the right is a 'Refresh' button.

In the main area, a filter bar is set to 'customer*'. Below it, under 'Selected fields', there is a dropdown menu with the option '? _source' selected. Under 'Available fields', there are several fields listed: '_id', '_index', '_score', '_type', and 'name'. The 'name' field has a checkmark icon next to it, indicating it is selected.

A results panel displays 2 hits:

_source
> name: John Doe 1 _id: 1 _type: _doc _index: customer _score: 0
> name: John Doe 2 _id: 2 _type: _doc _index: customer _score: 0

ELK: Filebeat + Redis

Run ELK

```
sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name elk sebp/elk
```

Setup / Run File Beat for Redis

```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.2-linux-x86_64.tar.gz  
tar xzvf filebeat-7.4.2-linux-x86_64.tar.gz  
.filebeat modules enable redis  
.filebeat setup  
.filebeat -e
```

<https://gist.github.com/diegopacheco/e35fb0adceb34b54c4dc4d304d686cd5>

ELK: Filebeat + Redis: Enable slowlog tracing



Commands Clients Documentation Community Download Modules Support

SLOWLOG subcommand [argument]

Available since 2.2.12.

This command is used in order to read and reset the Redis slow queries log.

Redis slow log overview

The Redis Slow Log is a system to log queries that exceeded a specified execution time. The execution time does not include I/O operations like talking with the client, sending the reply and so forth, but just the time needed to actually execute the command (this is the only stage of command execution where the thread is blocked and can not serve other requests in the meantime).

You can configure the slow log with two parameters: *slowlog-log-slower-than* tells Redis what is the execution time, in microseconds, to exceed in order for the command to get logged. Note that a negative number disables the slow log, while a value of zero forces the logging of every command. *slowlog-max-len* is the length of the slow log. The minimum value is zero. When a new command is logged and the slow log is already at its maximum length, the oldest one is removed from the queue of logged commands in order to make space.

The configuration can be done by editing `redis.conf` or while the server is running using the [CONFIG GET](#) and [CONFIG SET](#) commands.

Reading the slow log

Related commands

- [BGREWRITEAOF](#)
- [BGSAVE](#)
- [CLIENT GETNAME](#)
- [CLIENT ID](#)
- [CLIENT KILL](#)
- [CLIENT LIST](#)
- [CLIENT PAUSE](#)
- [CLIENT REPLY](#)
- [CLIENT SETNAME](#)
- [CLIENT UNBLOCK](#)
- [COMMAND](#)
- [COMMAND COUNT](#)
- [COMMAND GETKEYS](#)
- [COMMAND INFO](#)
- [CONFIG GET](#)
- [CONFIG RESETSTAT](#)
- [CONFIG REWRITE](#)
- [CONFIG SET](#)
- [DBSIZE](#)
- [DEBUG OBJECT](#)
- [DEBUG SEGFAULT](#)
- [FLUSHALL](#)
- [FLUSHDB](#)
- [INFO](#)

ELK: Filebeat + Redis: Enable slowlog tracing

The screenshot shows a terminal window with three tabs:

- Filebeat configuration: ./filebeat -e
- Docker run command: sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it...
- Redis CLI: redis-cli

The Redis CLI tab contains the following output:

```
127.0.0.1:6379> CONFIG SET slowlog-log-slower-than 0
OK
127.0.0.1:6379> SLOWLOG get
1) 1) (integer) 42
   2) (integer) 1576235809
   3) (integer) 16
   4) 1) "CONFIG"
      2) "SET"
      3) "slowlog-log-slower-than"
      4) "0"
   5) "127.0.0.1:52640"
   6) ""
2) 1) (integer) 41
   2) (integer) 1576235808
   3) (integer) 5
   4) 1) "SLOWLOG"
      2) "RESET"
   5) "127.0.0.1:55956"
   6) ""
127.0.0.1:6379>
```

ELK: Filebeat + Redis

```
./filebeat -e
File Edit View Search Terminal Tabs Help
./filebeat -e      sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it... diego@4winds: ~/bin/filebeat-7.4.2-linux-x86_64
2019-12-13T08:02:38.163-0300    INFO  [monitoring]  log/log.go:145 Non-zero metrics in the last 30s      {"monitoring": {"metrics": {"beat": {"cpu": {"system": {"ticks": 40, "time": {"ms": 8}}, "total": {"ticks": 120, "time": {"ms": 14}, "value": 120}, "user": {"ticks": 80, "time": {"ms": 6}}}, "handles": {"limit": {"hard": 65000, "soft": 65000}, "open": 15}, "info": {"ephemeral_id": "b2f81448-ddb1-4ccb-af27-5a325457fc4e", "uptime": {"ms": 90042}}, "memstats": {"gc_next": 8052672, "memory_alloc": 6129936, "memory_total": 12801816}, "runtime": {"goroutines": 33}}, "filebeat": {"harvester": {"open_files": 0, "running": 0}}, "libbeat": {"config": {"module": {"running": 0}}, "pipeline": {"clients": 4, "events": {"active": 0}}}, "registrar": {"states": {"current": 0}}, "system": {"load": {"1": 1.54, "15": 1.73, "5": 1.6, "norm": {"1": 0.1925, "15": 0.2163, "5": 0.2}}}}}
2019-12-13T08:03:08.163-0300    INFO  [monitoring]  log/log.go:145 Non-zero metrics in the last 30s      {"monitoring": {"metrics": {"beat": {"cpu": {"system": {"ticks": 60, "time": {"ms": 15}}, "total": {"ticks": 140, "time": {"ms": 20}}, "value": 140}, "user": {"ticks": 80, "time": {"ms": 5}}}, "handles": {"limit": {"hard": 65000, "soft": 65000}, "open": 6}, "info": {"ephemeral_id": "b2f81448-ddb1-4ccb-af27-5a325457fc4e", "uptime": {"ms": 120044}}, "memstats": {"gc_next": 7602784, "memory_alloc": 6265400, "memory_total": 13142104}, "runtime": {"goroutines": 33}}, "filebeat": {"harvester": {"open_files": 0, "running": 0}}, "libbeat": {"config": {"module": {"running": 0}}, "pipeline": {"clients": 4, "events": {"active": 0}}}, "registrar": {"states": {"current": 0}}, "system": {"load": {"1": 1.11, "15": 1.69, "5": 1.49, "norm": {"1": 0.1388, "15": 0.2113, "5": 0.1863}}}}}
2019-12-13T08:03:38.164-0300    INFO  [monitoring]  log/log.go:145 Non-zero metrics in the last 30s      {"monitoring": {"metrics": {"beat": {"cpu": {"system": {"ticks": 60, "time": {"ms": 4}}, "total": {"ticks": 150, "time": {"ms": 14}}, "value": 150}, "user": {"ticks": 90, "time": {"ms": 10}}}, "handles": {"limit": {"hard": 65000, "soft": 65000}, "open": 9}, "info": {"ephemeral_id": "b2f81448-ddb1-4ccb-af27-5a325457fc4e", "uptime": {"ms": 150043}}, "memstats": {"gc_next": 7602784, "memory_alloc": 4147720, "memory_total": 13488912}, "runtime": {"goroutines": 33}}, "filebeat": {"harvester": {"open_files": 0, "running": 0}}, "libbeat": {"config": {"module": {"running": 0}}, "pipeline": {"clients": 4, "events": {"active": 0}}}, "registrar": {"states": {"current": 0}}, "system": {"load": {"1": 1.09, "15": 1.67, "5": 1.44, "norm": {"1": 0.1363, "15": 0.2088, "5": 0.18}}}}}
2019-12-13T08:04:08.162-0300    INFO  [monitoring]  log/log.go:145 Non-zero metrics in the last 30s      {"monitoring": {"metrics": {"beat": {"cpu": {"system": {"ticks": 70, "time": {"ms": 11}}, "total": {"ticks": 160, "time": {"ms": 14}}, "value": 160}, "user": {"ticks": 90, "time": {"ms": 3}}}, "handles": {"limit": {"hard": 65000, "soft": 65000}, "open": 12}, "info": {"ephemeral_id": "b2f81448-ddb1-4ccb-af27-5a325457fc4e", "uptime": {"ms": 180043}}, "memstats": {"gc_next": 7602784, "memory_alloc": 4663288, "memory_total": 14004480}, "runtime": {"goroutines": 33}}, "filebeat": {"harvester": {"open_files": 0, "running": 0}}, "libbeat": {"config": {"module": {"running": 0}}, "pipeline": {"clients": 4, "events": {"active": 0}}}, "registrar": {"states": {"current": 0}}, "system": {"load": {"1": 1, "15": 1.64, "5": 1.38, "norm": {"1": 0.125, "15": 0.205, "5": 0.1725}}}}}
2019-12-13T08:04:38.162-0300    INFO  [monitoring]  log/log.go:145 Non-zero metrics in the last 30s      {"monitoring": {"metrics": {"beat": {"cpu": {"system": {"ticks": 80, "time": {"ms": 8}}, "total": {"ticks": 180, "time": {"ms": 11}}, "value": 180}, "user": {"ticks": 100, "time": {"ms": 3}}}, "handles": {"limit": {"hard": 65000, "soft": 65000}, "open": 15}, "info": {"ephemeral_id": "b2f81448-ddb1-4ccb-af27-5a325457fc4e", "uptime": {"ms": 210043}}, "memstats": {"gc_next": 7602784, "memory_alloc": 5004568, "memory_total": 14345760, "rss": 770048}, "runtime": {"goroutines": 33}}, "filebeat": {"harvester": {"open_files": 0, "running": 0}}, "libbeat": {"config": {"module": {"running": 0}}, "pipeline": {"clients": 4, "events": {"active": 0}}}, "registrar": {"states": {"current": 0}}, "system": {"load": {"1": 0.95, "15": 1.61, "5": 1.33, "norm": {"1": 0.1188, "15": 0.2013, "5": 0.1663}}}}}}
```

<https://gist.github.com/diegopacheco/e35fb0adceb34b54c4dc4d304d686cd5>

ELK: Filebeat + Redis: Documentation inside ELK

localhost:5601/app/kibana#/home/tutorial/redisLogs?_g=()

Home / Add data / Redis logs

Redis logs

The `redis` Filebeat module parses error and slow logs created by Redis. For Redis to write error logs, make sure the `logfile` option, from the Redis configuration file, is set to `redis-server.log`. The slow logs are read directly from Redis via the `SLOWLOG` command. For Redis to record slow logs, make sure the `slowlog-log-slower-than` option is set. Note that the `slowlog` fileset is experimental. [Learn more.](#)

[View exported fields](#)

Self managed Elastic Cloud

Getting Started

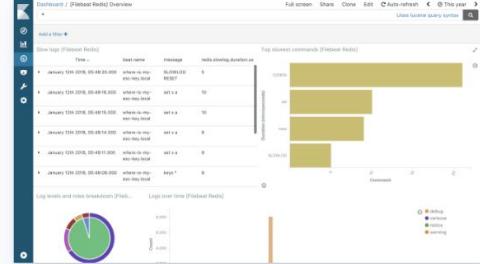
macOS DEB RPM Windows

1 Download and install Filebeat

First time using Filebeat? See the [Getting Started Guide](#).

`curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.1.0-darwin-x86_64.tgz`

[Copy snippet](#)



ELK: Filebeat + Redis: Check if is all working!

The screenshot shows the Kibana interface with a sidebar of icons and a main content area. The top navigation bar includes a Kibana icon, a document icon, and links to 'Home', 'Add data', and 'Redis logs'. The sidebar has 14 icons corresponding to various Kibana features.

Step 4: Start Filebeat

The setup command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

```
./filebeat setup  
./filebeat -e
```

Copy snippet

Module status

Check that data is received from the Filebeat redis module

Data successfully received from this module

Check data

When all steps are complete, you're ready to explore your data.

Redis logs dashboard

ELK: Filebeat + Redis: Data in ELK

localhost:5601/app/kibana#/discover?_g=(refreshInterval:(pause:0,value:0),time:(from:now-15h,to:now))&_a=(columns:!(_source),index:'filebeat-*',interval:auto,query:(language:kuery,query:redis),sort:[{!(_id:desc)}],size:50,version:6)

Discover

	Time	_source
t _id		
t _index		
# _score		
t _type		
t agent.ephemeral_id	> Dec 13, 2019 @ 08:14:58.000	event.module: redis input.type: redis service.type: redis @timestamp: Dec 13, 2019 @ 08:14:58.000 message: SLOWLOG RESET redis.slowlog.duration.us: 6 redis.slowlog.id: 19 redis.slowlog.cmd: SLOWLOG redis.slowlog.key: RESET ecs.version: 1.1.0 host.name: 4winds host.id: 658cbb0cefae4a8685fd05a0ac9ae4eb host.containerized: false host.hostname: 4winds host.architecture: x86_64 host.os.family: debian host.os.name: Ubuntu host.os.kernel: 4.15.0-72-
t agent.hostname		
t agent.id		
t agent.type		
t agent.version	> Dec 13, 2019 @ 08:14:50.000	input.type: redis event.module: redis service.type: redis @timestamp: Dec 13, 2019 @ 08:14:50.000 agent.ephemeral_id: b2f81448-dbdb1-4ccb-af27-5a325457fc4e agent.hostname: 4winds agent.id: b2ef3bed-d5ca-401c-b272-380b832d9a14 agent.version: 7.4.2 agent.type: filebeat ecs.version: 1.1.0 host.architecture: x86_64 host.os.codename: bionic host.os.platform: ubuntu host.os.version: 18.04.3 LTS (Bionic Beaver) host.os.family: debian host.os.name: Ubuntu host.os.kernel: 4.15.0-72-generic
t event.dataset		
t event.module	> Dec 13, 2019 @ 08:14:48.000	input.type: redis event.module: redis service.type: redis @timestamp: Dec 13, 2019 @ 08:14:48.000 message: SLOWLOG RESET redis.slowlog.duration.us: 6 redis.slowlog.id: 16 redis.slowlog.cmd: SLOWLOG redis.slowlog.key: RESET ecs.version: 1.1.0 event.created: Dec 13, 2019 @ 08:14:58.318 event.dataset: redis.slowlog fileset.name: slowlog host.name: 4winds host.os.family: debian host.os.name: Ubuntu host.os.kernel: 4.15.0-72-generic host.os.codename: bionic
t host.architecture		
t host.containerized		
t host.hostname	> Dec 13, 2019 @ 08:14:47.000	event.module: redis input.type: redis service.type: redis @timestamp: Dec 13, 2019 @ 08:14:47.000 event.created: Dec 13, 2019 @ 08:14:48.316 event.dataset: redis.slowlog fileset.name: slowlog
t host.id		

Time @timestamp per 10 minutes

ELK: Java Application ~ Spring Boot 2x + Actuator + Micrometer



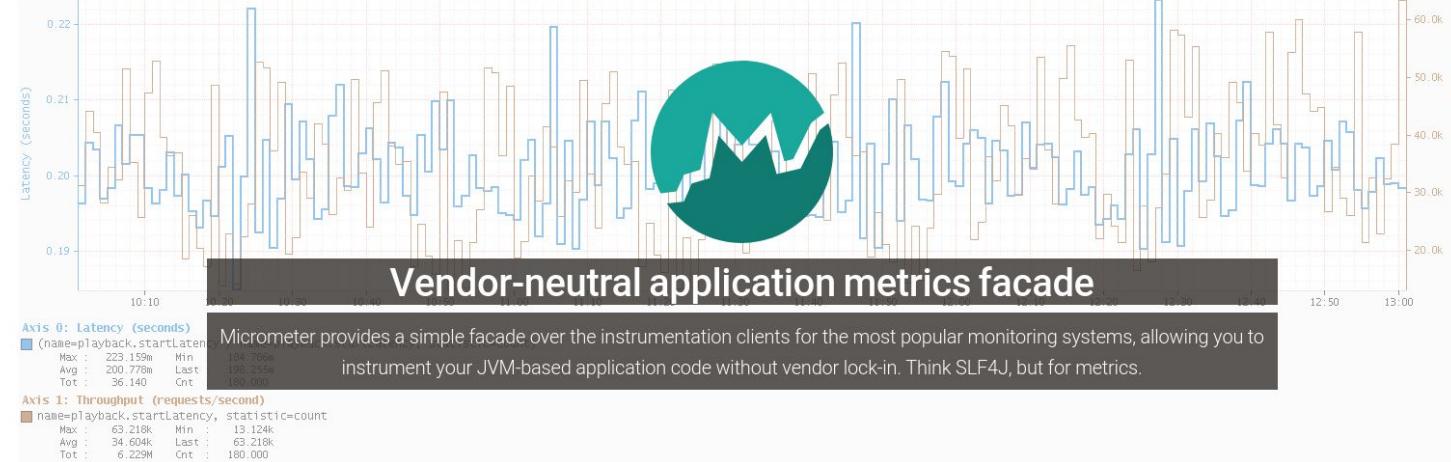
MICROMETER
application monitoring

[Documentation](#)

[GitHub](#)

[Twitter](#)

[Slack](#)



Dimensional Metrics

Micrometer provides vendor-neutral interfaces for **timers**, **gauges**, **counters**, **distribution summaries**, and **long task timers** with a dimensional data model that, when paired with a dimensional monitoring system, allows for efficient access to a particular named metric with the ability to drill down across its dimensions.



Pre-configured Bindings

Out-of-the-box instrumentation of caches, the class loader, garbage collection, processor utilization, thread pools, and more tailored to actionable insight.



Integrated into Spring

Starting with Spring Boot 2.0, Micrometer is the instrumentation library powering the delivery of application metrics from Spring. Support is ported back to Boot 1.x through an additional library dependency.

ELK: Java Application ~ Spring Boot 2x + Actuator + Micrometer

build.gradle

```
34 dependencies {  
35     compile("org.springframework.boot:spring-boot-starter-web")  
36     compile("org.springframework.boot:spring-boot-starter-actuator")  
37     compile("io.micrometer:micrometer-registry-elastic")  
38  
39     testImplementation 'org.junit.jupiter:junit-jupiter-api:5.5.2'  
40     testRuntimeOnly 'org.junit.jupiter:junit-jupiter-engine:5.5.2'  
41 }
```

src/main/resources/application.properties

src > main > resources > application.properties

```
1 management.endpoints.web.exposure.include=*  
2 management.metrics.export.elastic=true  
3 management.metrics.export.elastic.index: java.springboot2x_metrics  
4 management.metrics.export.elastic.host=http://localhost:9200
```

ELK: Java Application ~ Spring Boot 2x + Actuator + Micrometer

MainController.java

```
src > main > java > springboot2x > controller > MainController.java > ...
1 package springboot2x.controller;
2
3 import org.springframework.web.bind.annotation.RequestMapping;
4 import org.springframework.web.bind.annotation.RestController;
5
6 @RestController
7 public class MainController{
8
9     @RequestMapping("/")
10    public String index() {
11        return "Greetings from Spring Boot 2x!";
12    }
13
14 }
```

ELK: Java Application ~ Spring Boot 2x + Actuator + Micrometer

Application.java ->

```
src > main > java > springboot2x > app > Application.java > ...
  6  import org.springframework.boot.SpringApplication;
  7  import org.springframework.boot.autoconfigure.SpringBootApplication;
  8  import org.springframework.context.ApplicationContext;
  9  import org.springframework.context.annotation.Bean;
 10
 11 @SpringBootApplication(scanBasePackages = "springboot2x")
 12 public class Application {
 13
 14     Run | Debug
 15     public static void main(String[] args) {
 16         SpringApplication.run(Application.class, args);
 17     }
 18
 19     @Bean
 20     public CommandLineRunner commandLineRunner(ApplicationContext ctx) {
 21         return args -> {
 22             System.out.println("Let's inspect the beans provided by Spring Boot:");
 23             String[] beanNames = ctx.getBeanDefinitionNames();
 24             Arrays.sort(beanNames);
 25             for (String beanName : beanNames) {
 26                 System.out.println(beanName);
 27             }
 28         };
 29     }
 30 }
```

ELK: Java Application ~ Spring Boot 2x + Actuator + Micrometer

```
$ ./gradlew bootRun
```

```
diego@4winds ~ -/github/diegopacheco/sw-design-course/src/java/java-ELK master ① ./gradlew bootRun SIGINT(2) 16:58:14 ~ 0.80G 1.54 ijd
> Task :bootRun
.
( ( ) [ ] { } [ ] ( ) ) )
=====
:: Spring Boot :: (v2.2.2.RELEASE)

2020-01-02 17:58:17.351 INFO 2669 --- [           main] springboot2x.app.Application      : Starting Application on 4winds with PID 2669 (/home/diego/github/diegopacheco/sw-design-course/src/java/java-ELK)
2020-01-02 17:58:17.354 INFO 2669 --- [           main] springboot2x.app.Application      : No active profile set, falling back to default profiles: default
2020-01-02 17:58:18.433 INFO 2669 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer : Tomcat initialized with port(s): 8080 (http)
2020-01-02 17:58:18.442 INFO 2669 --- [           main] o.apache.catalina.core.StandardService : Starting service [Tomcat]
2020-01-02 17:58:18.443 INFO 2669 --- [           main] org.apache.catalina.core.StandardEngine : Starting Servlet engine: [Apache Tomcat/9.0.29]
2020-01-02 17:58:18.499 INFO 2669 --- [           main] o.a.c.c.C.[Tomcat].[localhost].[/] : Initializing Spring embedded WebApplicationContext
2020-01-02 17:58:18.500 INFO 2669 --- [           main] o.s.web.context.ContextLoader       : Root WebApplicationContext: initialization completed in 1100 ms
2020-01-02 17:58:18.525 INFO 2669 --- [           main] i.m.elastic.ElasticMeterRegistry    : publishing metrics to elastic every 1m
2020-01-02 17:58:18.850 INFO 2669 --- [           main] o.s.s.concurrent.ThreadPoolTaskExecutor: Initializing ExecutorService 'applicationTaskExecutor'
2020-01-02 17:58:19.048 INFO 2669 --- [           main] o.s.b.a.e.web.EndpointLinksResolver : Exposing 13 endpoint(s) beneath base path '/actuator'
2020-01-02 17:58:19.120 INFO 2669 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer : Tomcat started on port(s): 8080 (http) with context path ''
2020-01-02 17:58:19.123 INFO 2669 --- [           main] springboot2x.app.Application      : Started Application in 2.12 seconds (JVM running for 2.487)

Let's inspect the beans provided by Spring Boot:
application
applicationTaskExecutor
basicErrorHandler
beanNameHandlerMapping
beanNameViewResolver
beansEndpoint
cachesEndpoint
cachesEndpointWebExtension
characterEncodingFilter
classLoaderMetrics
commandLineRunner
conditionsReportEndpoint
configurationPropertiesReportEndpoint
controllerEndpointDiscoverer
controllerEndpointHandlerMapping
```

ELK: Java Application ~ Spring Boot 2x + Actuator + Micrometer

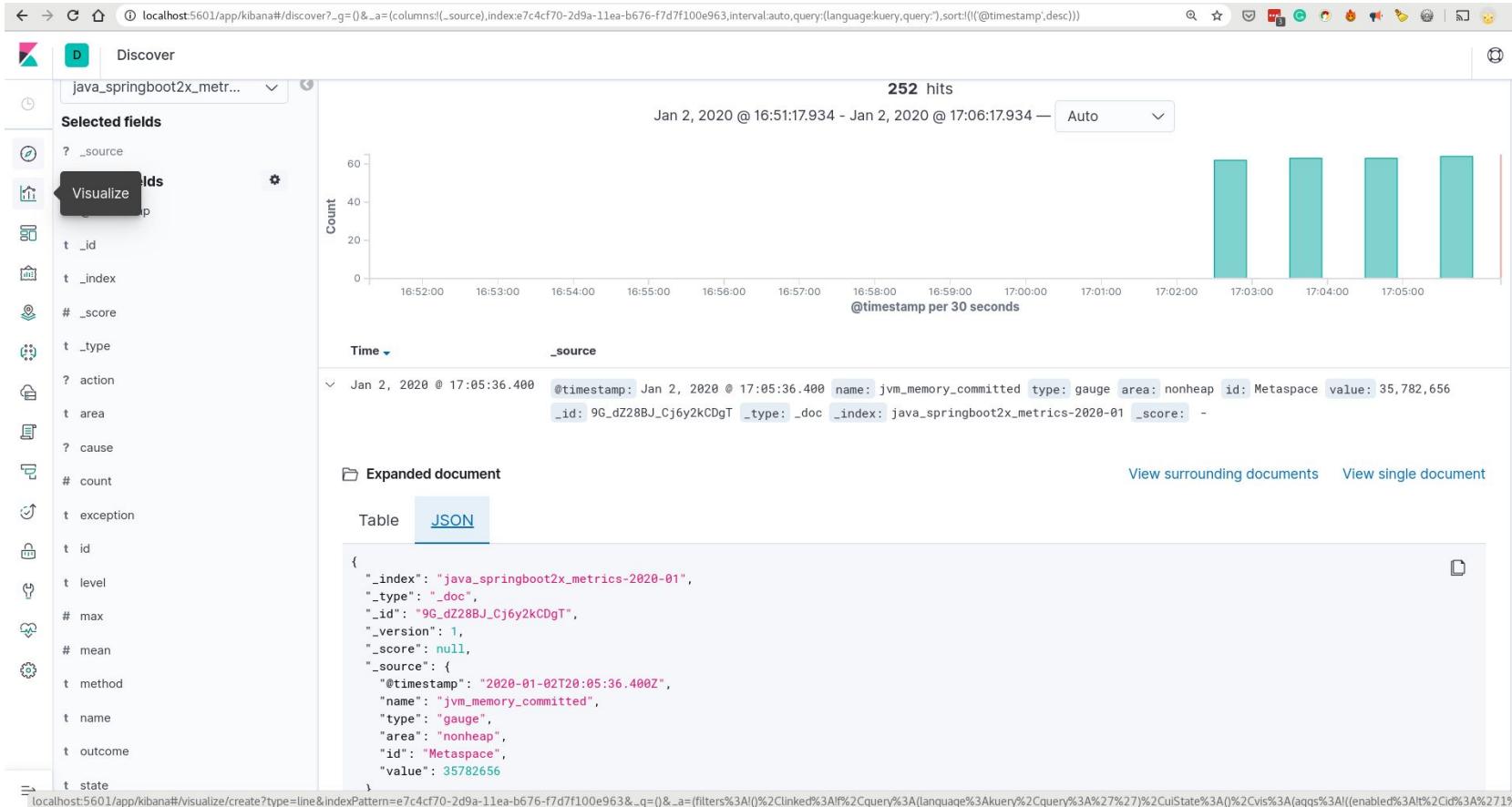
```
$ ./gradlew bootRun
```

```
servletEndpointRegistrar
servletExposeExcludePropertyEndpointFilter
servletMappingDescriptionProvider
servletWebChildContextFactory
servletWebServerFactoryCustomizer
simpleControllerHandlerAdapter
spring.http.org.springframework.boot.autoconfigure.http.HttpProperties
spring.info.org.springframework.boot.autoconfigure.info.ProjectInfoProperties
spring.jackson.org.springframework.boot.autoconfigure.jackson.JacksonProperties
spring.mvc.org.springframework.boot.autoconfigure.web.servlet.WebMvcProperties
spring.resources.org.springframework.boot.autoconfigure.web.ResourceProperties
spring.security.oauth2.resourceserver.org.springframework.boot.autoconfigure.security.oauth2.resource OAuth2ResourceServerProperties
spring.servlet.multipart.org.springframework.boot.autoconfigure.web.servlet.MultipartProperties
spring.task.execution.org.springframework.boot.autoconfigure.task.TaskExecutionProperties
spring.task.scheduling.org.springframework.boot.autoconfigure.task.TaskSchedulingProperties
standardJacksonObjectMapperBuilderCustomizer
stringHttpMessageConverter
taskExecutorBuilder
taskSchedulerBuilder
tomcatMetricsBinder
tomcatServletWebServerFactory
tomcatServletWebServerFactoryCustomizer
tomcatWebServerFactoryCustomizer
uptimeMetrics
viewControllerHandlerMapping
viewResolver
webEndpointDiscoverer
webEndpointPathMapper
webEndpointServletHandlerMapping
webExposeExcludePropertyEndpointFilter
webMvcMetricsFilter
webMvcTagsProvider
webServerFactoryCustomizerBeanPostProcessor
websocketServletWebServerCustomizer
welcomePageHandlerMapping
2020-01-02 18:01:44.292 INFO 3391 --- [nio-8080-exec-1] o.a.c.c.C.[Tomcat].[localhost].[]          : Initializing Spring DispatcherServlet 'dispatcherServlet'
2020-01-02 18:01:44.292 INFO 3391 --- [nio-8080-exec-1] o.s.web.servlet.DispatcherServlet        : Initializing Servlet 'dispatcherServlet'
2020-01-02 18:01:44.297 INFO 3391 --- [nio-8080-exec-1] o.s.web.servlet.DispatcherServlet        : Completed initialization in 5 ms
<=====> 95% EXECUTING [13m 0s]
> :bootRun
```

ELK: Java Application ~ Spring Boot 2x + Actuator + Micrometer

```
// 20200102170237
// http://localhost:8080/actuator/metrics
{
  "names": [
    "jvm.memory.max",
    "jvm.threads.states",
    "process.files.max",
    "jvm.gc.memory.promoted",
    "system.load.average.1m",
    "jvm.memory.used",
    "jvm.gc.max.data.size",
    "jvm.memory.committed",
    "system.cpu.count",
    "logback.events",
    "jvm.buffer.memory.used",
    "tomcat.sessions.created",
    "jvm.threads.daemon",
    "system.cpu.usage",
    "jvm.gc.memory.allocated",
    "tomcat.sessions.expired",
    "jvm.threads.live",
    "jvm.threads.peak",
    "process.uptime",
    "tomcat.sessions.rejected",
    "process.cpu.usage",
    "http.server.requests",
    "jvm.classes.loaded",
    "jvm.classes.unloaded",
    "tomcat.sessions.active.current",
    "tomcat.sessions.alive.max",
    "jvm.gc.live.data.size",
    ...
  ]
}
```

ELK: Java Application ~ Spring Boot 2x + Actuator + Micrometer



ELK: Java Application ~ Sending Logs ~ Running Logstash

src/main/resources/logback.xml

```
src > main > resources > logback.xml
1   <configuration>
2     <appender name="STDOUT" class="ch.qos.logback.core.ConsoleAppender">
3       <encoder>
4         <pattern>%-4relative [%thread] %-5level %logger{35} - %msg %n</pattern>
5       </encoder>
6     </appender>
7     <appender name="STASH" class="ch.qos.logback.core.rolling.RollingFileAppender">
8       <file>logs/springboot2xapp.log</file>
9       <rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
10         <fileNamePattern>logs/springboot2xapp.%d{yyyy-MM-dd}.log</fileNamePattern>
11         <maxHistory>7</maxHistory>
12       </rollingPolicy>
13       <encoder class="net.logstash.logback.encoder.LogstashEncoder"/>
14     </appender>
15     <root level="INFO">
16       <appender-ref ref="STASH" />
17       <appender-ref ref="STDOUT" />
18     </root>
19   </configuration>
```

ELK: Java Application ~ Sending Logs ~ Running Logstash

build.gradle

```
34 dependencies {  
35     compile("org.springframework.boot:spring-boot-starter-web")  
36     compile("org.springframework.boot:spring-boot-starter-actuator")  
37     compile("io.micrometer:micrometer-registry-elastic")  
38     compile("net.logstash.logback:logstash-logback-encoder:4.11")  
39     compile("ch.qos.logback:logback-classic")  
40  
41     testImplementation 'org.junit.jupiter:junit-jupiter-api:5.5.2'  
42     testRuntimeOnly 'org.junit.jupiter:junit-jupiter-engine:5.5.2'  
43 }
```

ELK: Java Application ~ Sending Logs ~ Running Logstash

build.gradle

```
src > main > java > springboot2x > controller > MainController.java > ...
1 package springboot2x.controller;
2
3 import org.slf4j.Logger;
4 import org.slf4j.LoggerFactory;
5 import org.springframework.web.bind.annotation.RequestMapping;
6 import org.springframework.web.bind.annotation.RestController;
7
8 @RestController
9 public class MainController{
10
11     private static final Logger LOGGER = LoggerFactory.getLogger(MainController.class);
12
13     @RequestMapping("/")
14     public String index() {
15         LOGGER.info("Serving a success request. Dont do this in PROD!");
16         return "Greetings from Spring Boot 2x!";
17     }
18
19 }
```

ELK: Java Application ~ Sending Logs ~ Running Logstash

```
wget https://artifacts.elastic.co/downloads/logstash/logstash-7.5.1.tar.gz
```

```
tar -zcvf logstash-7.5.1.tar.gz
```

```
rm -rf logstash-7.5.1.tar.gz
```

logback.conf

```
logstash-conf > ⚙ logback.conf
1   input {
2     file {
3       path => "/home/diego/github/diegopacheco/sw-design-course/src/java/java-ELK/logs/*.log"
4       codec => "json"
5       type => "logback"
6     }
7   }
8
9   output {
10    if [type]==="logback" {
11      elasticsearch {
12        hosts => [ "localhost:9200" ]
13        index => "logback-%{+YYYY.MM.dd}"
14      }
15    }
16 }
```

ELK: Java Application ~ Sending Logs ~ Running Logstash

bin/logstash -f \$APP_PATH/logstash-conf/logback.conf

```
diego@winds:~/bin$ ./logstash-7.5.1/bin/logstash -f /home/diego/github/diegopacheco/sw-design-course/src/java/ELK/logstash-conf/logback.conf
Thread.exclusive is deprecated, use Thread::Mutex
Sending Logstash logs to /home/diego/bin/logstash-7.5.1/logs which is now configured via log4j2.properties
[2020-01-02T18:45:58,504][INFO ][logstash.setting.writabledirectory] Creating directory {:setting=>"path.queue", :path=>"/home/diego/bin/logstash-7.5.1/data/queue"}
[2020-01-02T18:45:58,745][INFO ][logstash.setting.writabledirectory] Creating directory {:setting=>"path.dead_letter_queue", :path=>"/home/diego/bin/logstash-7.5.1/data/dead_letter_queue"}
[2020-01-02T18:45:59,579][WARN ][logstash.config.source.multilocal] Ignoring the 'pipelines.yml' file because modules or command line options are specified
[2020-01-02T18:45:59,600][INFO ][logstash.runner] Starting Logstash {"logstash.version"=>"7.5.1"}
[2020-01-02T18:45:59,662][INFO ][logstash.agent] No persistent UUID file found. Generating new UUID {:uuid=>"2d08321e-5a04-4651-8665-6b38c511d38c", :path=>"/home/diego/bin/logstash-7.5.1/data/uuid"}
[2020-01-02T18:46:04,436][INFO ][org.reflections.Reflections] Reflections took 90 ms to scan 1 urls, producing 20 keys and 40 values
[2020-01-02T18:46:07,293][INFO ][logstash.outputs.elasticsearch][main] Elasticsearch pool URLs updated {:changes=>{:removed=>[], :added=>[http://localhost:9200/]}}
[2020-01-02T18:46:07,694][WARN ][logstash.outputs.elasticsearch][main] Restored connection to ES instance {:url=>"http://localhost:9200/"}
[2020-01-02T18:46:07,792][INFO ][logstash.outputs.elasticsearch][main] ES Output version determined {:es_version=>7}
[2020-01-02T18:46:07,801][WARN ][logstash.outputs.elasticsearch][main] Detected a 6.x and above cluster: the `type` event field won't be used to determine the document _type
{:es_version=>7}
[2020-01-02T18:46:08,084][INFO ][logstash.outputs.elasticsearch][main] New Elasticsearch output {:class=>"LogStash::Outputs::ElasticSearch", :hosts=>["//localhost:9200"]}
[2020-01-02T18:46:08,297][INFO ][logstash.outputs.elasticsearch][main] Using default mapping template
[2020-01-02T18:46:08,390][WARN ][org.logstash.instrument.metrics.gauge.LazyDelegatingGauge][main] A gauge metric of an unknown type (org.jruby.specialized.RubyArrayOneObject) has been created for key: cluster_uuids. This may result in invalid serialization. It is recommended to log an issue to the responsible developer/development team.
[2020-01-02T18:46:08,400][INFO ][logstash.javapipeline][main] Starting pipeline {:pipeline_id=>"main", "pipeline.workers"=>8, "pipeline.batch.size"=>125, "pipeline.batch.delay"=>50, "pipeline.max_inflight"=>1000, "pipeline.sources"=>["/home/diego/github/diegopacheco/sw-design-course/src/java/ELK/logstash-conf/logback.conf"], :thread=>#<Thread:>0x55c552fb run>}
[2020-01-02T18:46:08,565][INFO ][logstash.outputs.elasticsearch][main] Attempting to install template {:manage_template=>{"index_patterns"=>"logstash-*", "version"=>60001, "settings"=>{"index.refresh_interval"=>"5s", "number_of_shards"=>1}, "mappings"=>{"dynamic_templates"=>[{"message_field"=>{"path_match"=>"message", "match_mapping_type"=>"string", "mapping"=>{"type"=>"text", "norms"=>false}}, {"string_fields"=>{"match"=>"*", "match_mapping_type"=>"string", "mapping"=>{"type"=>"text", "norms"=>false, "fields"=>{"keyword"=>{"type"=>"keyword", "ignore_above"=>256}}}}, "properties"=>{@timestamp=>{"type"=>"date"}, "@version"=>{"type"=>"keyword"}, "geoip"=>{"dynamic"=>true, "properties"=>{"ip"=>{"type"=>"ip"}, "location"=>{"type"=>"geo_point"}, "latitude"=>{"type"=>"half_float"}, "longitude"=>{"type"=>"half_float"}}}}}
[2020-01-02T18:46:08,640][INFO ][logstash.outputs.elasticsearch][main] Installing elasticsearch template to _template/logstash
[2020-01-02T18:46:09,640][INFO ][logstash.inputs.file][main] No since_db_path set, generating one based on the "path" setting {:since_db_path=>"/home/diego/bin/logstash-7.5.1/data/plugins/inputs/file/.since_db_36b99b31c7cd7c034f4188e711adba4c", :path=>["/home/diego/github/diegopacheco/sw-design-course/src/java/ELK/logs/*.log"]}
[2020-01-02T18:46:09,841][INFO ][logstash.javapipeline][main] Pipeline started {"pipeline.id"=>"main"}
[2020-01-02T18:46:10,120][INFO ][logstash.agent] Pipelines running {:count=>1, :running_pipelines=>[]}
[2020-01-02T18:46:10,207][INFO ][filewatch.observingtail][main] START, creating Discoverer, Watch with file and since_db collections
[2020-01-02T18:46:11,274][INFO ][logstash.agent] Successfully started Logstash API endpoint {:port=>9600}
```

ELK: Java Application ~ Sending Logs ~ Running Logstash

You can see there is a new ES log - proof that it works. You can create a index on Kibana now.

```
diego@4winds ➜ -/github/diegopacheco/sw-design-course/src/java/java-ELK/logstash-conf ➜ ✘ master ❁ ? curl http://localhost:9200/_cat/indices
yellow open java.springboot2x.metrics-2020-01 tF8zKTVfSeOjAMq3azRiMw 1 1 2175 0 313.6kb 313.6kb
green open .kibana.task_manager_1 cTFiwgXJRCs6VcUoqKLbZw 1 0 2 0 46.4kb 46.4kb
green open .apm-agent-configuration AJRH9-TNRv00EoseXeEpTA 1 0 0 0 283b 283b
yellow open logback-2020.01.02 zqaJAt6USXiUWB9gCtAKaw 1 1 5 0 18.3kb 18.3kb
yellow open metrics-2020-01 MDzDrDiISC6oaCqaAm-YUg 1 1 2089 0 241.3kb 241.3kb
green open .kibana_1 S0gKVLM6Q-CGq-2GCsjc0A 1 0 26 6 164.8kb 164.8kb
```

ELK: Java Application ~ Sending Logs ~ Running Logstash

The screenshot shows the Kibana Discover interface. On the left is a sidebar with various icons and a list of fields: host, level, #_level_value, logger_name, message, path, thread_name, type. The main area shows a single document expanded. The document has a timestamp of Jan 2, 2020 @ 17:52:50.447 and is of type _doc. It contains the following JSON:

```
{  
  "_index": "logback-2020.01.02",  
  "_type": "_doc",  
  "_id": "um8IaG8BJ_Cj6y2kSEAG",  
  "_version": 1,  
  "_score": null,  
  "_source": {  
    "host": "4winds",  
    "type": "logback",  
    "message": "Serving a success request. Dont do this in PROD!",  
    "@timestamp": "2020-01-02T20:52:50.447Z",  
    "@version": 1,  
    "thread_name": "http-nio-8080-exec-8",  
    "logger_name": "springboot2x.controller.MainController",  
    "level_value": 20000,  
    "path": "/home/diego/github/diegopacheco/sw-design-course/src/java/java-ELK/logs/springboot2xapp.log",  
    "level": "INFO"  
  },  
  "fields": {  
    "@timestamp": [  
      "2020-01-02T20:52:50.447Z"  
    ]  
  },  
  "sort": [  
    1577998370447  
  ]  
}
```

Below the expanded document, there are two more documents listed: Jan 2, 2020 @ 17:52:50.398 and Jan 2, 2020 @ 17:52:50.151.

Observability

Splunk



16 matching events

Timeline: zoom in zoom out Scale: linear log 1 bar = 1 minute

2:18 PM Thu Jul 15 2010 2:19 PM 2:20 PM 2:21 PM 2:22 PM 2:23 PM

21 fields | Pick fields

Selected fields (3)

- host (1)
- source (2)
- sourceType (1)

Other interesting fields (8)

- index (1)
- linecount (n) (1)
- pid (n) (5)
- process (5)
- punct (6)
- splunk_server (1)
- timeendpos (n) (1)
- timestartpos (n) (1)

All 21 Fields

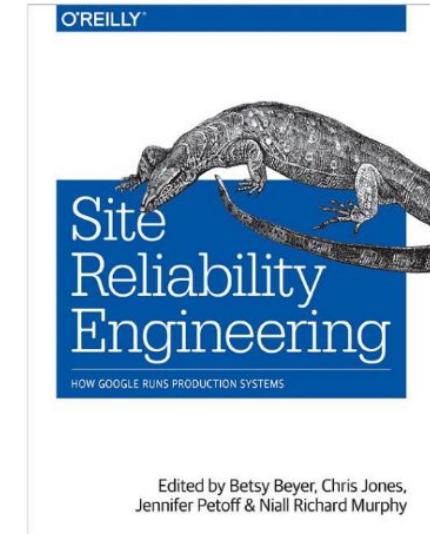
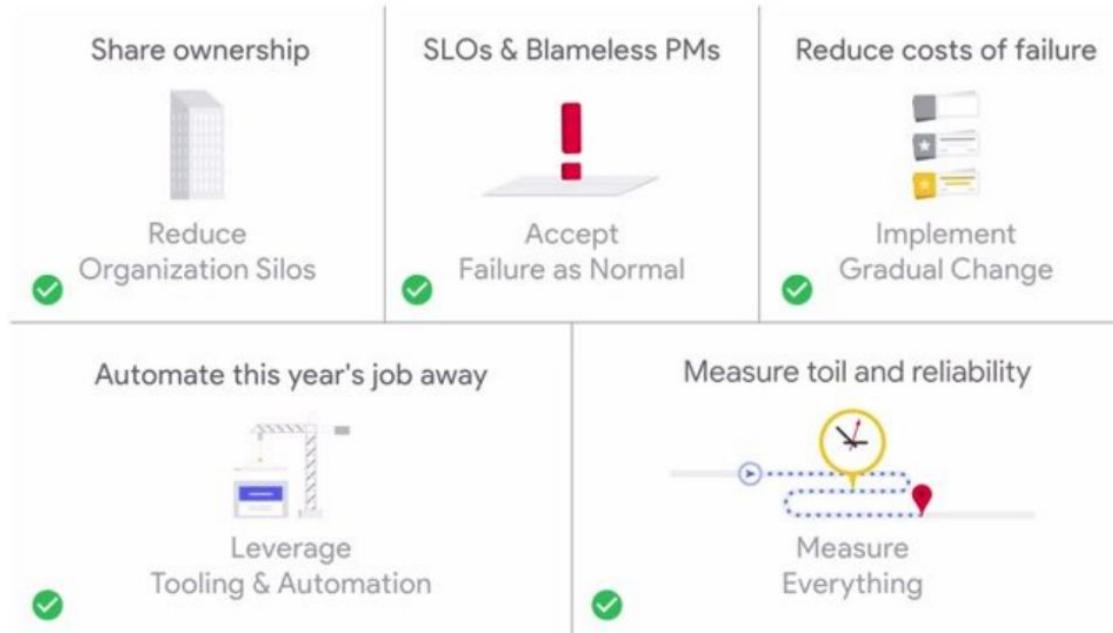
16 events from 2:18 PM to 2:23 PM on Thursday, July 15, 2010

Results per page 10

Time	Event
Jul 15 14:23:02 192.168.1.102 abnev-ip1 apsd[51]: <APSCourier: 0x1078c0>: Stream error occurred for <APSTCPStream: 0x112980>; Error Domain=NSPOSIXErrorDomain Code=68 "Operation could not be completed. Operation timed out"	host=192.168.1.102 sourceType=syslog source=/private/var/log/system.log.0.bz2
Jul 15 14:23:02 192.168.1.102 abnev-ip1 apsd[51]: <APSCourier: 0x1078c0>: Stream error occurred for <APSTCPStream: 0x112980>; Error Domain=NSPOSIXErrorDomain Code=68 "Operation could not be completed. Operation timed out"	host=192.168.1.102 sourceType=syslog source=/private/var/log/system.log
Jul 15 14:22:53 192.168.1.102 abnev-ip1 sshd[327]: USER_PROCESS: 327 ttys001	host=192.168.1.102 sourceType=syslog source=/private/var/log/system.log.0.bz2
Jul 15 14:22:53 192.168.1.102 abnev-ip1 sshd[327]: USER_PROCESS: 327 ttys001	host=192.168.1.102 sourceType=syslog source=/private/var/log/system.log
Jul 15 14:22:43 192.168.1.102 abnev-ip1 sshd[182]: DEAD_PROCESS: 183 ttys001	host=192.168.1.102 sourceType=syslog source=/private/var/log/system.log.0.bz2
Jul 15 14:22:43 192.168.1.102 abnev-ip1 sshd[182]: DEAD_PROCESS: 183 ttys001	host=192.168.1.102 sourceType=syslog source=/private/var/log/system.log
Jul 15 14:18:22 192.168.1.102 abnev-ip1 com.apple.itunesstored[313]: MS:Warning: nil class argument	host=192.168.1.102 sourceType=syslog source=/private/var/log/system.log.0.bz2
Jul 15 14:18:22 192.168.1.102 abnev-ip1 itunesstored[313]: MS:Notice: Loading /Library/MobileSubstrate/DynamicLibraries/iNoRotate.dylib	host=192.168.1.102 sourceType=syslog source=/private/var/log/system.log.0.bz2

Observability

SRE



Observability

Google - How to Develop SRE?

What Makes SRE, SRE?

Simple:

- Hire only coders
- Have an SLA for your service
- Measure and report performance against SLA
- Use Error Budgets and gate launches on them
- Common staffing pool for SRE and DEV
- Excess Ops work overflows to DEV team
- Cap SRE operational load at 50%
- Share 5% of ops work with DEV team
- Oncall teams at least 8 people, or 6x2
- Maximum of 2 events per oncall shift.
- Post mortem for every event
- Post mortems are blameless and focus on process and technology, not people

Observability

Characteristics of Toil

- Manual
- Repetitive
- Automatable
- Tactical
- Devoid of long-term value

Overhead

Not toil

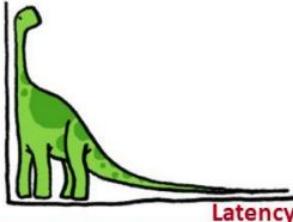
- Email
- Expense reports
- Meetings
- Traveling

Observability

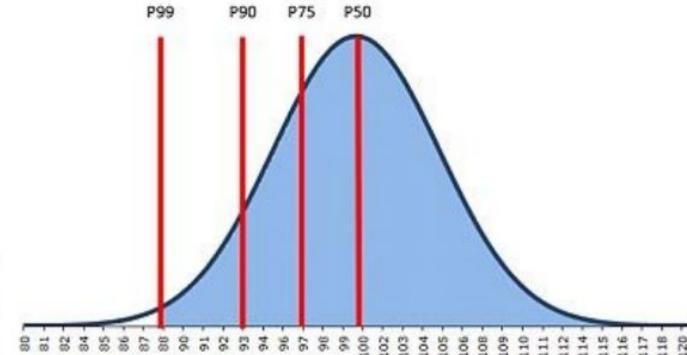
Tail Latency

Low Latency for All Users

- **Reduce tail latency** (high-percentile response time)
- Reducing average latency is not sufficient

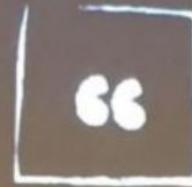


Commercial search engine reduces 99th-percentile latency



Observability

Reliability and Availability!



A service is available if users
cannot tell there was an outage.

Observability



Prometheus



- Long Term Remote Storage for Prometheus
- Support prometheus query API
- Support for Grafana
- Outperform InfluxDB and TimescaleDB by 20x more performance on inserts / selects
- Uses 10x less ram than influxDB
- High Data Compression - 70x more compression than TimescaleDB
- Easy Operation (Easy backup to S3) Ingestion via: Prometheus, InfluxDB, Graphite APIs
- OSS Cluster

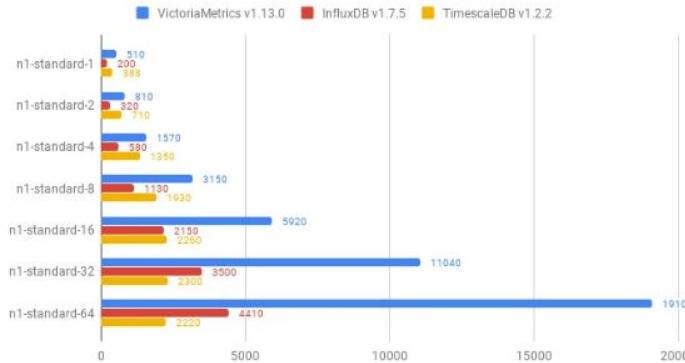
Observability



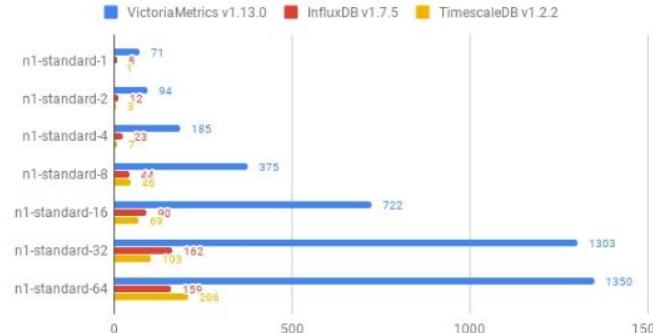
VICTORIA
METRICS

Benchmarks

Ingestion rate, thousands of data points / sec (higher is better)



double-groupby-1, clients=vCPUs, rpm (higher is better)



```
docker run --network=host -it --rm -v
/tmp/victoria-metrics-data:/victoria-metrics-data -p 8428:8428
```

File Edit View Search Terminal Help

```
2019-11-27T03:59:56.769+0000    info    VictoriaMetrics@/lib/storage/storage.go:568    loading MetricID->MetricName cache from "/victoria-metrics-data/cache/metricID_metricName"...
2019-11-27T03:59:56.771+0000    info    VictoriaMetrics@/lib/storage/storage.go:573    loaded MetricID->MetricName cache from "/victoria-metrics-data/cache/metricID metricName" in 1.211597ms; entriesCount: 0; sizeBytes: 0
2019-11-27T03:59:56.771+0000    info    VictoriaMetrics@/lib/storage/storage.go:484    loading curr_hour_metric_ids from "/victoria-metrics-data/cache/curr_hour_metric_ids"...
2019-11-27T03:59:56.771+0000    info    VictoriaMetrics@/lib/storage/storage.go:487    nothing to load from "/victoria-metrics-data/cache/curr_hour_metric_ids"
2019-11-27T03:59:56.771+0000    info    VictoriaMetrics@/lib/storage/storage.go:484    loading prev_hour_metric_ids from "/victoria-metrics-data/cache/prev_hour_metric_ids"...
2019-11-27T03:59:56.771+0000    info    VictoriaMetrics@/lib/storage/storage.go:487    nothing to load from "/victoria-metrics-data/cache/prev_hour_metric_ids"
2019-11-27T03:59:56.779+0000    info    VictoriaMetrics@/lib/mergeset/table.go:156    opening table "/victoria-metrics-data/indexdb/15DAE8FDDC6C8C47"...
2019-11-27T03:59:56.791+0000    info    VictoriaMetrics@/lib/mergeset/table.go:190    table "/victoria-metrics-data/indexdb/15DAE8FDDC6C8C47" has been opened in 11.793625ms; partsCount: 0; blocksCount: 0, itemsCount: 0; sizeBytes: 0
2019-11-27T03:59:56.793+0000    info    VictoriaMetrics@/lib/mergeset/table.go:156    opening table "/victoria-metrics-data/indexdb/15DAE8FDDC6C8C46"...
2019-11-27T03:59:56.813+0000    info    VictoriaMetrics@/lib/mergeset/table.go:190    table "/victoria-metrics-data/indexdb/15DAE8FDDC6C8C46" has been opened in 20.10401ms; partsCount: 0; blocksCount: 0, itemsCount: 0; sizeBytes: 0
2019-11-27T03:59:56.838+0000    info    VictoriaMetrics@/app/vmstorage/main.go:65    2019-11-27T03:59:56.838+0000    info    VictoriaMetrics@/app/vmstorage/main.go:65    successfully opened storage "victoria-metrics-data" in 90.428265ms; partsCount: 0; blocksCount: 0; rowsCount: 0; sizeBytes: 0
2019-11-27T03:59:56.842+0000    info    VictoriaMetrics@/app/vmselect/promql/rollup_result_cache.go:50    2019-11-27T03:59:56.842+0000    info    VictoriaMetrics@/app/vmselect/promql/rollup_result_cache.go:50    loading rollupResult cache from "victoria-metrics-data/cache/rollupResult"...
2019-11-27T03:59:56.849+0000    info    VictoriaMetrics@/app/vmselect/promql/rollup_result_cache.go:76    2019-11-27T03:59:56.849+0000    info    VictoriaMetrics@/app/vmselect/promql/rollup_result_cache.go:76    loaded rollupResult cache from "victoria-metrics-data/cache/rollupResult" in 7.165587ms; entriesCount: 0, sizeBytes: 0
2019-11-27T03:59:56.849+0000    info    VictoriaMetrics@/app/victoria-metrics/main.go:31    2019-11-27T03:59:56.850+0000    info    VictoriaMetrics@/lib/httpserver/httpserver.go:63    started VictoriaMetrics in 101.808002ms
2019-11-27T03:59:56.850+0000    info    VictoriaMetrics@/lib/httpserver/httpserver.go:63    starting http server at http://:8428/
2019-11-27T03:59:56.850+0000    info    VictoriaMetrics@/lib/httpserver/httpserver.go:64    pprof handlers are exposed at http://:8428/debug/pprof/
```

Observability - curl -v http://127.0.0.1:8428/metrics



```
diego@4winds: ~
File Edit View Search Terminal Tabs Help
docker run -it --rm -v /tmp/victoria-metrics-data:/victoria-metrics-data -p
diego@4winds: ~
diego@4winds: ~ 20:17:34 7.49G 1.24 [ml]
curl -v http://127.0.0.1:8428/metrics
* Trying 127.0.0.1...
* TCP_NODELAY set
* Connected to 127.0.0.1 (127.0.0.1) port 8428 (#0)
> GET /metrics HTTP/1.1
> Host: 127.0.0.1:8428
> User-Agent: curl/7.58.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Content-Type: text/plain
< Date: Wed, 27 Nov 2019 04:17:46 GMT
< Transfer-Encoding: chunked
<
vm_active_merges{type="indexdb"} 0
vm_active_merges{type="storage/big"} 0
vm_active_merges{type="storage/small"} 0
vm_assisted_merges_total{type="indexdb"} 0
vm_assisted_merges_total{type="storage/small"} 0
vm_blocks{type="indexdb"} 0
vm_blocks{type="storage/big"} 0
vm_blocks{type="storage/small"} 0
vm_cache_collisions_total{type="storage/metricName"} 0
vm_cache_collisions_total{type="storage/tsid"} 0
vm_cache_entries{type="indexdb/dataBlocks"} 0
vm_cache_entries{type="indexdb/indexBlocks"} 0
vm_cache_entries{type="indexdb/tagFilters"} 0
vm_cache_entries{type="indexdb/uselessTagFilters"} 0
vm_cache_entries{type="promql/parse"} 0
vm_cache_entries{type="promql/recover"} 0
```

*docker run --network=host --rm --name=grafana -p 300
grafana/grafana*



```
File Edit View Search Terminal Tabs Help
docker run --rm --name=grafana -p 3000:3000 grafana/grafana
docker run -it --rm -v /tmp/victoria-metrics-data:/victoria-metrics-data -p
docker run --rm --name=grafana -p 3000:3000 grafana/grafana

t=2019-11-27T04:23:58+0000 lvl=info msg="Executing migration" logger=migrator id="add unique index user_auth_token.prev_auth_token"
t=2019-11-27T04:23:58+0000 lvl=info msg="Executing migration" logger=migrator id="create cache_data_table"
t=2019-11-27T04:23:58+0000 lvl=info msg="Executing migration" logger=migrator id="add unique index cache_data.cache_key"
t=2019-11-27T04:23:58+0000 lvl=info msg="Created default admin" logger=sqlstore user=admin
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing HTTPServer" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing OSSLicensingService" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing SearchService" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing RemoteCache" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing QuotaService" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing ServerLockService" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing UserAuthTokenService" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing PluginManager" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Starting plugin search" logger=plugins
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing RenderingService" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing AlertEngine" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing DatasourceCacheService" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing HooksService" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing LoginService" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing InternalMetricsService" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing TracingService" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing UsageStatsService" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing CleanUpService" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing NotificationService" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing provisioningServiceImpl" logger=server
t=2019-11-27T04:23:58+0000 lvl=info msg="Backend rendering via phantomJS" logger=rendering
t=2019-11-27T04:23:58+0000 lvl=warn msg="phantomJS is deprecated and will be removed in a future release. You should consider migrating from phantomJS to grafana-image-renderer plugin." logger=rendering
t=2019-11-27T04:23:58+0000 lvl=info msg="Initializing Stream Manager"
t=2019-11-27T04:23:58+0000 lvl=info msg="HTTP Server Listen" logger=http.server address=[::]:3000 protocol=http subUrl= socket=
```



Prometheus

docker run --network=host --rm --name=prometheus -v \$(pwd)/prometheus.yml:/etc/prometheus/prometheus.yml -p 9090:9090 prom/prometheus

```
File Edit View Search Terminal Tabs Help
docker run --rm --name=prometheus -v -p 9090:9090 prom/prometheus
diego@4winds ~ docker run --rm -name=prometheus -v $(pwd)/prometheus.yml:/etc/prometheus/prometheus.yml -p 9090:9090 prom/prometheus
level=info ts=2019-11-27T05:24:10.469Z caller=main.go:296 msg="no time or size retention was set so using the default time retention" duration=15d
level=info ts=2019-11-27T05:24:10.469Z caller=main.go:332 msg="Starting Prometheus" version="(version=2.14.0, branch=HEAD, revision=edeb7a44cbf745f1d8be4eaef215e79e651bfe19)"
level=info ts=2019-11-27T05:24:10.469Z caller=main.go:333 build_context="(go=golang 1.13.4, user=root@df2327081015, date=20191111-14:27:12)"
level=info ts=2019-11-27T05:24:10.469Z caller=main.go:334 host_details="(Linux 4.15.0-70-generic #79-Ubuntu SMP Tue Nov 12 10:36:11 UTC 2019 x86_64 0920a9ab70d3 (none))"
level=info ts=2019-11-27T05:24:10.469Z caller=main.go:335 fd_limits="(soft=1048576, hard=1048576)"
level=info ts=2019-11-27T05:24:10.469Z caller=main.go:336 vm_limits="(soft=unlimited, hard=unlimited)"
level=info ts=2019-11-27T05:24:10.471Z caller=main.go:657 msg="Starting TSDB ..."
level=info ts=2019-11-27T05:24:10.471Z caller=web.go:496 component=web msg="Start listening for connections" address=0.0.0.0:9090
level=info ts=2019-11-27T05:24:10.472Z caller=head.go:535 component=tsdb msg="replaying WAL, this may take awhile"
level=info ts=2019-11-27T05:24:10.472Z caller=head.go:583 component=tsdb msg="WAL segment loaded" segment=0 maxSegment=0
level=info ts=2019-11-27T05:24:10.472Z caller=main.go:672 fs_type=EXT4_SUPER_MAGIC
level=info ts=2019-11-27T05:24:10.472Z caller=main.go:673 msg="TSDB started"
level=info ts=2019-11-27T05:24:10.472Z caller=main.go:743 msg="Loading configuration file" filename=/etc/prometheus/prometheus.yml
ts=2019-11-27T05:24:10.481Z caller=dedupe.go:111 component=remote level=info queue=0:http://localhost:8428/api/v1/write msg="starting WAL watcher" queue=0:http://localhost:8428/api/v1/write
level=info ts=2019-11-27T05:24:10.482Z caller=main.go:771 msg="Completed loading of configuration file" filename=/etc/prometheus/prometheus.yml
level=info ts=2019-11-27T05:24:10.482Z caller=main.go:626 msg="Server is ready to receive web requests."
```

curl http://localhost:9090/metrics



```
diego@4winds: ~
File Edit View Search Terminal Tabs Help
docker run --network host --name=victoria -it --rm ... docker run --network host -rm --name=grafana ... docker run --network=host --rm --name=promet... diego@4winds: ~ 21:27:43 ~ 8.03G 1.01 dd
diego@4winds ~ ~ ~ curl http://localhost:9090/metrics
# HELP go_gc_duration_seconds A summary of the GC invocation durations.
# TYPE go_gc_duration_seconds summary
go_gc_duration_seconds{quantile="0"} 1.8341e-05
go_gc_duration_seconds{quantile="0.25"} 2.4125e-05
go_gc_duration_seconds{quantile="0.5"} 3.0861e-05
go_gc_duration_seconds{quantile="0.75"} 0.000180502
go_gc_duration_seconds{quantile="1"} 0.00026871
go_gc_duration_seconds_sum 0.001200924
go_gc_duration_seconds_count 14
# HELP go_goroutines Number of goroutines that currently exist.
# TYPE go_goroutines gauge
go_goroutines 40
# HELP go_info Information about the Go environment.
# TYPE go_info gauge
go_info{version="go1.13.4"} 1
# HELP go_memstats_alloc_bytes Number of bytes allocated and still in use.
# TYPE go_memstats_alloc_bytes gauge
go_memstats_alloc_bytes 1.5434584e+07
# HELP go_memstats_alloc_bytes_total Total number of bytes allocated, even if freed.
# TYPE go_memstats_alloc_bytes_total counter
go_memstats_alloc_bytes_total 1.15540824e+08
# HELP go_memstats_buck_hash_sys_bytes Number of bytes used by the profiling bucket hash table.
# TYPE go_memstats_buck_hash_sys_bytes gauge
go_memstats_buck_hash_sys_bytes 1.452296e+06
# HELP go_memstats_frees_total Total number of frees.
# TYPE go_memstats_frees_total counter
go_memstats_frees_total 136319
# HELP go_memstats_gc_cpu_fraction The fraction of this program's available CPU time used by the GC since the program started.
```

Prometheus Redis Exporter



```
./redis_exporter

File Edit View Search Terminal Tabs Help
docker run --network host --name=vi... docker run --network host --rm --na... docker run --network=host --rm --na... ./redis_exporter redis-cli
diego@4winds ~ go get github.com/oliver006/redis_exporter
diego@4winds ~ cd $GOPATH/src/github.com/oliver006/redis_exporter
diego@4winds ~ /bin/golang/src/github.com/oliver006/redis_exporter & master . v1.3.4 go build
diego@4winds ~ /bin/golang/src/github.com/oliver006/redis_exporter & master . v1.3.4 ./redis_exporter
INFO[0000] Redis Metrics Exporter <<< filled in by build >>> build date: <<< filled in by build >>> sha1: <<< filled in by build >>> Go: go1.12.9 GOOS: linux GOARCH: amd64
INFO[0000] Providing metrics at :9121/metrics
```

```
redis-cli

File Edit View Search Terminal Tabs Help
docker run --network host --name=vi... docker run --network host --rm --na... docker run --network=host --rm --na... ./redis_exporter redis-cli
127.0.0.1:6379> keys *
1) "Dephy"
2) "myhash"
3) "mylist"
4) "cache-1"
5) "myset:_rand_int_"
6) "my_key"
7) "cache-empresa-orsegups"
8) "counter:_rand_int_"
9) "kcount"
10) "key:_rand_int_"
11) "k"
12) "Ike"
13) "x"
14) "Garfield"
15) "Melina"
127.0.0.1:6379> get x
"10"
127.0.0.1:6379>
```

https://github.com/oliver006/redis_exporter

Prometheus Redis Exporter



```
diego@4winds: ~
File Edit View Search Terminal Tabs Help
diego@4winds ~ bat prometheus.yml diego@4winds ~
File: prometheus.yml
1 remote_write:
2   - url: http://localhost:8428/api/v1/write
3     queue_config:
4       max_samples_per_send: 10000
5       max_shards: 30
6     scrape_configs:
7       - job_name: redis_exporter
8         static_configs:
9           - targets: ['localhost:9121']
diego@4winds ~
22:04:11 7.77G 0.68 [!]
22:04:19 7.87G 0.68 [!]
```

```
docker run --network=host --rm --name=prometheus -v
$(pwd)/prometheus.yml:/etc/prometheus/prometheus.yml -p
9090:9090 prom/prometheus
```

Prometheus UI



localhost:9090/new/graph?g0.expr=redis_commands_total&g0.tab=1&g0.stacked=0&g0.range_input=1h

Prometheus Alerts Graph Status ▾ Help Classic UI

Enable query history

redis_commands_total G Execute

Table Graph

Evaluation time < >

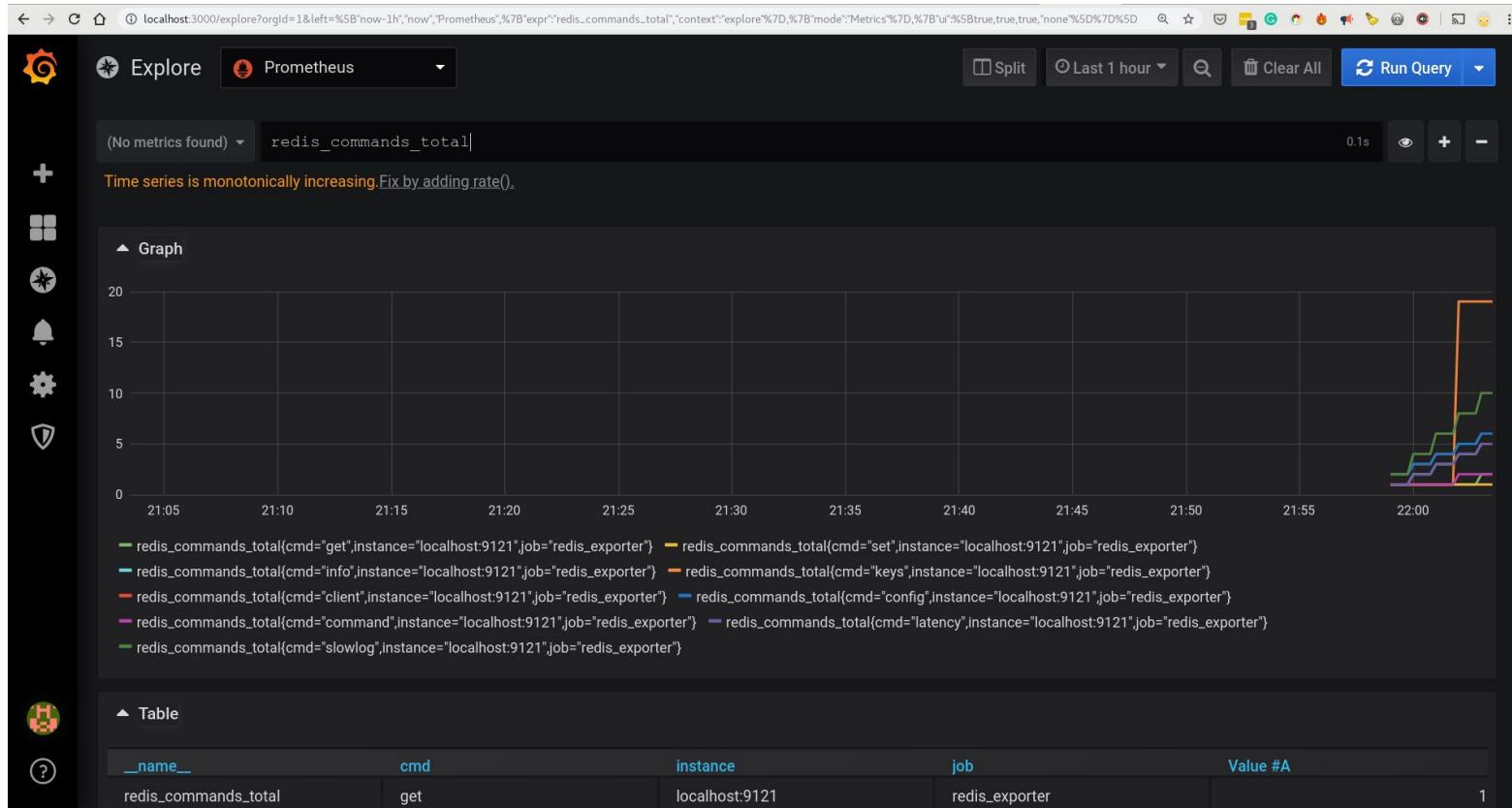
Load time: 34ms Resolution: 14s Result series: 9

redis_commands_total{cmd="client", instance="localhost:9121", job="redis_exporter"}	5
redis_commands_total{cmd="command", instance="localhost:9121", job="redis_exporter"}	2
redis_commands_total{cmd="config", instance="localhost:9121", job="redis_exporter"}	5
redis_commands_total{cmd="get", instance="localhost:9121", job="redis_exporter"}	1
redis_commands_total{cmd="info", instance="localhost:9121", job="redis_exporter"}	4
redis_commands_total{cmd="keys", instance="localhost:9121", job="redis_exporter"}	19
redis_commands_total{cmd="latency", instance="localhost:9121", job="redis_exporter"}	4
redis_commands_total{cmd="set", instance="localhost:9121", job="redis_exporter"}	1
redis_commands_total{cmd="slowlog", instance="localhost:9121", job="redis_exporter"}	8

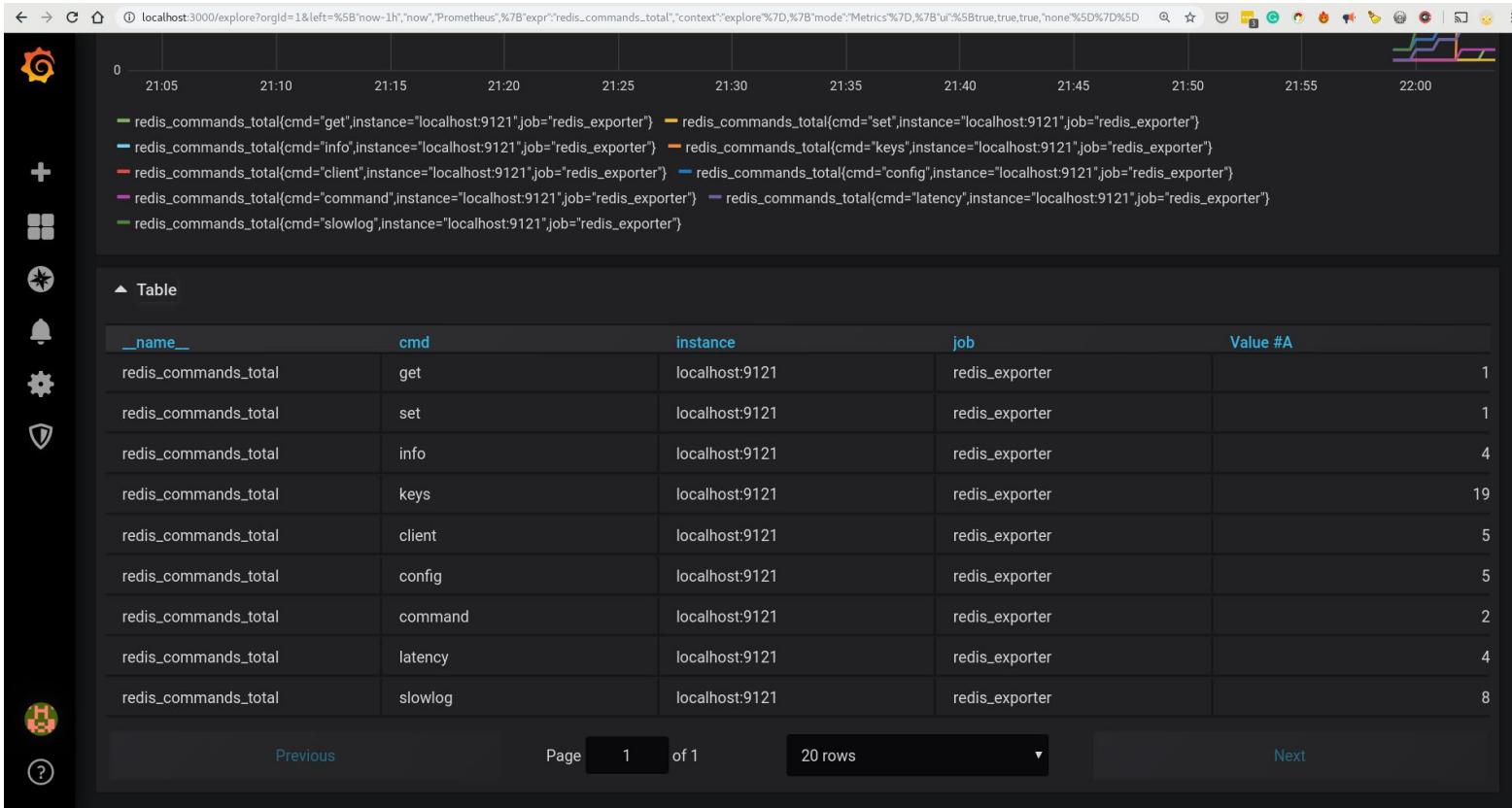
Remove Panel

Add Panel

Grafana UI



Grafana UI



Prometheus Exporters



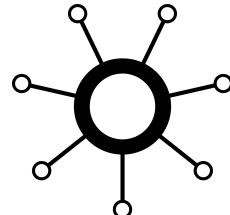
redis



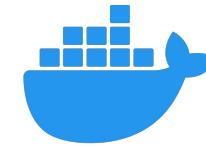
elasticsearch



NGINX



Amazon CloudWatch



docker



Grafana Dashboard for Victoria Metrics



Grafana Labs Grafana Products Open Source Learn Downloads Login Contact Us

All dashboards » VictoriaMetrics

VictoriaMetrics by VictoriaMetrics

DASHBOARD Overview for single node VictoriaMetrics v1.29.0 or higher
Last updated: 15 days ago

Downloads: 339 Reviews: 0 Add your review!

Overview Revisions Reviews



VictoriaMetrics single-server overview

Requirements
VictoriaMetrics v1.29.0 or higher.
Use Prometheus datasource with Prometheus or VictoriaMetrics URL.

Description
Dashboard contains visualization of most useful metrics displaying current state and performance of the service. If you have suggestions, improvements or found a bug - feel free to add issue or add review to the dashboard.
More information about [VictoriaMetrics](#).
New [releases](#) and [images](#).

Get this dashboard:
10229
Copied! Click to copy again.

Download JSON
How do I import this dashboard?

Dependencies:

- GRAFANA 6.4.4
- GRAPH
- PROMETHEUS 1.0.0
- SINGLESTAT
- TABLE
- TEXT

Data Sources:

- PROMETHEUS

10229

<https://grafana.com/grafana/dashboards/10229>

Observability - Victoria Metrics Cluster

Clients

`vmselect` fully supports PromQL and can be used as Prometheus datasource in Grafana

Stateless

`vmselect` fetches and merges data from `vmstorage` during queries

Statefull

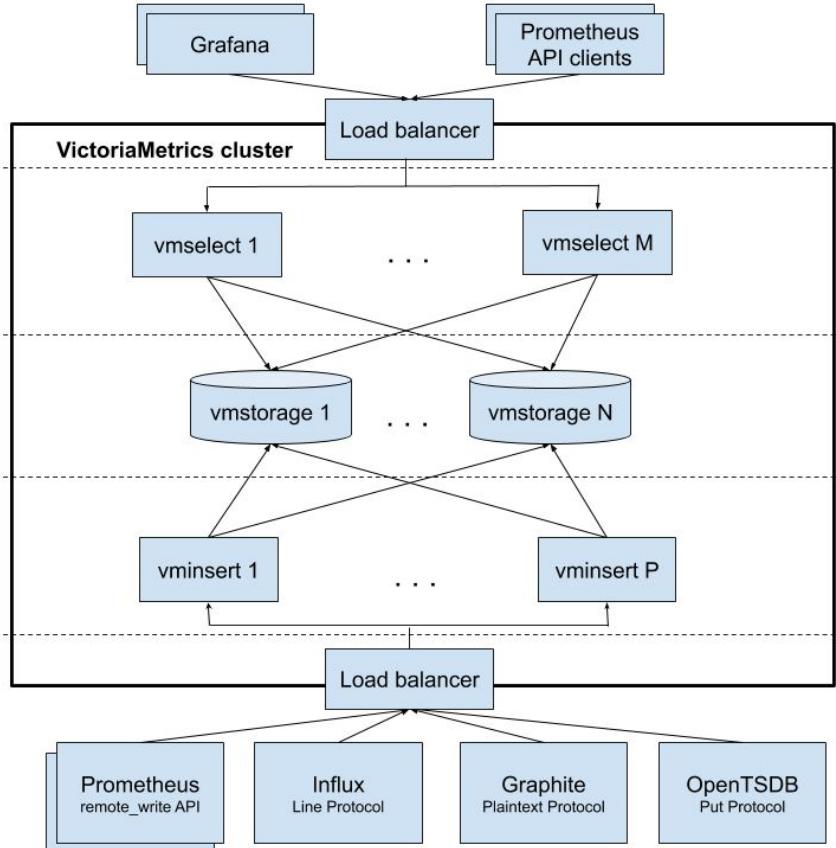
`vmstorage` stores time series data

Stateless

`vminsert` spreads time series across available `vmstorage` nodes

Writers

Multiple Prometheus instances may write data to VictoriaMetrics cluster
There is support for other ingestion protocols



Open Tracing

 OPENTRACING

DOCS

GUIDES

PROJECT

GET INVOLVED

GITHUB

BLOG

REGISTRY



SAY HI ON GITTER



```
bash

# Start Jaeger locally
$ docker run -d -p 5831:6831/udp -p 16686:16686 jaegertracing/all-in-one:latest
$ export DOCKER_IP=$(docker machine ip $(docker machine active))
$ cd $GOPATH/src

# Grab a simple, self contained OpenTracing example
$ go get github.com/opentracing/contrib/examples/go
$ cd github.com/opentracing/contrib/examples/go
$ go run ./trivial.go $DOCKER_IP

# Visualize the tracing instrumentation in Jaeger by
# clicking on 'Find Traces' in the UI
$ open http://$DOCKER_IP:16686/

# Read the source
$ vim trivial.go
```

Vendor-neutral APIs and
instrumentation for distributed tracing

Libraries available in 9 languages

[Go](#), [JavaScript](#), [Java](#), [Python](#), [Ruby](#), [PHP](#), [Objective-C](#), [C++](#), [C#](#)

The latest from our blog:

[OpenTracing on Kubernetes —get yer tracing for free](#)

Supported Tracers



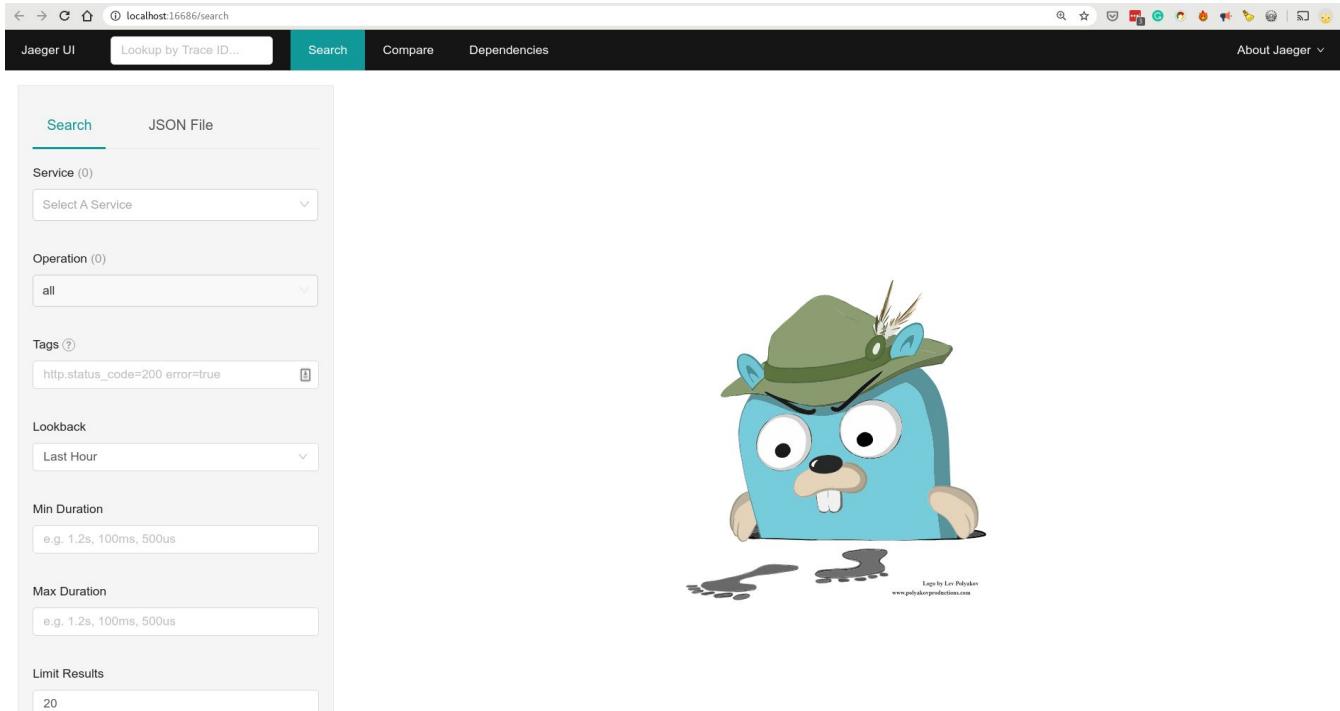
Supported Frameworks



<https://opentracing.io/>

Open Tracing - Java App ~ Run Jaeger

```
docker run --rm -it --network=host jaegertracing/all-in-one
```



The screenshot shows the Jaeger UI search interface at <http://localhost:16686/search>. The interface has a dark header with tabs for "Jaeger UI", "Lookup by Trace ID...", "Search", "Compare", and "Dependencies". The "Search" tab is active. On the left, there is a sidebar with the following sections and dropdowns:

- Service (0)**: Select A Service
- Operation (0)**: all
- Tags (?**): http.status_code=200 error=true
- Lookback**: Last Hour
- Min Duration**: e.g. 1.2s, 100ms, 500us
- Max Duration**: e.g. 1.2s, 100ms, 500us
- Limit Results**: 20

In the center, there is a large, friendly-looking blue gopher character wearing a green fedora hat with a feather. The gopher is looking slightly to the right. Below the gopher, the text "Logo by Lev Polyskin" and the URL "www.polyskinproductions.com" are visible.

<http://localhost:16686/search>

Open Tracing - Java App

build.gradle

```
33  
34 dependencies {  
35     compile("org.springframework.boot:spring-boot-starter-web")  
36     compile("org.springframework.boot:spring-boot-starter-actuator")  
37     compile("io.micrometer:micrometer-registry-elastic")  
38     compile("net.logstash.logback:logstash-logback-encoder:4.11")  
39     compile("ch.qos.logback:logback-classic")  
40     compile("io.opentracing.contrib:opentracing-spring-jaeger-web-starter:2.0.3")  
41  
42     testImplementation 'org.junit.jupiter:junit-jupiter-api:5.5.2'  
43     testRuntimeOnly 'org.junit.jupiter:junit-jupiter-engine:5.5.2'  
44 }
```

application.properties

```
Ξ application.properties ×  
  
src > main > resources > Ξ application.properties  
1 | spring.application.name=springboot2xapp  
2 | management.endpoints.web.exposure.include=*  
3 | management.metrics.export.elastic=true  
4 | management.metrics.export.elastic.index: java.springboot2x_metrics  
5 | management.metrics.export.elastic.host=http://localhost:9200
```

Open Tracing - Java App

localhost:16686/search?end=1578000378467000&limit=20&lookback=1h&maxDuration&minDuration&service=springboot2xapp&start=1577996778467000

Jaeger UI Lookup by Trace ID... Search Compare Dependencies About Jaeger

Search JSON File

Service (3) **springboot2xapp**

Operation (1) all

Tags http.status_code=200 error=true

Lookback Last Hour

Min Duration e.g. 1.2s, 100ms, 500us

Max Duration e.g. 1.2s, 100ms, 500us

Limit Results 20

Duration

Time

40ms
20ms

06:25:20 pm 06:25:30 pm 06:25:40 pm 06:25:50 pm

8 Traces Sort: Most Recent Deep Dependency Graph

Compare traces by selecting result items

springboot2xapp: index 4fb4871 6.01ms

1 Span **springboot2xapp (1)** Today | 6:25:59 pm
a few seconds ago

springboot2xapp: index 0d73e66 3.72ms

1 Span **springboot2xapp (1)** Today | 6:25:17 pm
a minute ago

springboot2xapp: index ccd6489 3.3ms

Open Tracing - Java App

Jaeger UI Lookup by Trace ID... Search Compare Dependencies About Jaeger ▾

◀ ▼ **springboot2xapp: index 4fb4871** Find... ⌂ ⌃ ⌄ ⌅ ⌆ ⌇ ⌈ ⌉ ⌋ ⌊ ⌊ ⌋ ⌃ ⌁ Trace Timeline ▾

Trace Start **January 2 2020, 18:25:59.138** | Duration **6.01ms** | Services **1** | Depth **1** | Total Spans **1**



Service & Operation 0ms 1.5ms 3ms 4.51ms 6.01ms

springboot2xapp index

index Service: **springboot2xapp** | Duration: **6.01ms** | Start Time: **0ms**

> **Tags:** component = java-web-servlet | http.method = GET | http.status_code = 200 | http.url = http://localhost:8080/ | internal.span.format = proto | sampler.param = true...

> **Process:** hostname = 4winds | ip = 127.0.1.1 | jaeger.version = Java-0.35.1

Logs (2)

3ms

event	"preHandle"
handler	"springboot2x.controller.MainController#index()"
handler.class_simple_name	"MainController"
handler.method_name	"index"

6ms

event	"afterCompletion"
handler	"springboot2x.controller.MainController#index()"

Log timestamps are relative to the start time of the full trace.

SpanID: 4fb4871770809145 ↗



Exercises

Constraints

1. You can use Java, Scala or Clojure as Language
2. You can use SpringBoot2x, Jetty or Netty as Server
3. You need to use Logback / ELK / Jaeger

Let's build a simple ecommerce

1. Build 2 microservices, first microservice will store items and do stock control. The microservice need to have 3 operations /add/\$item where you should have a name, description, photoURL and units at stock . Second endpoint need be able to retrieve an item by ID, last endpoint need to be able to update items on the stock /stock/\$ID (increase or decrease items). Second service need provide SALES so the sales microservices will call items/stock microservices in order to sales.
2. Add All logs in ELK
3. Add traces in Jaeger
4. Prodive custom metrics and add them in ELK create a dashboard showing: TOP sales, items that less less, salesman who sells more, items with less units on stock.



Observability

DIEGO PACHECO



Stack