Computer Systems & Network Administration

Lecture 15. System Monitoring & Network Monitoring

Reference: NYCU CSCC NASA

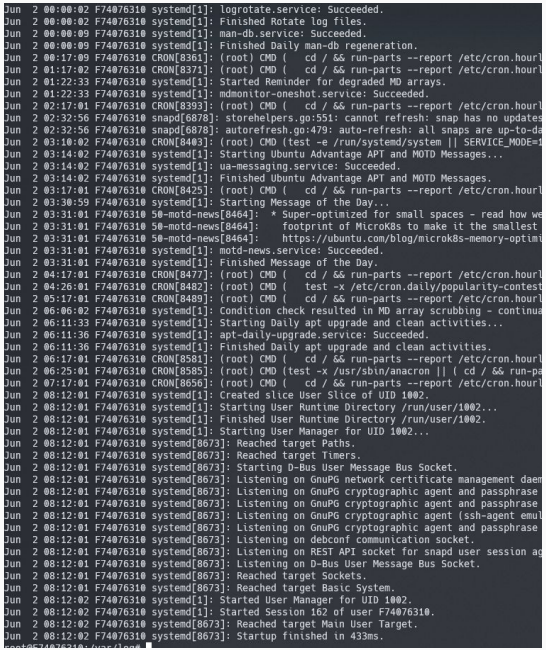
Outline

- Syslog & Log Rotate
- Time series Databases
- SNMP
- Grafana
- Log Aggregator
- Network Monitoring
- Monitoring Suite

Syslog & Log Rotate

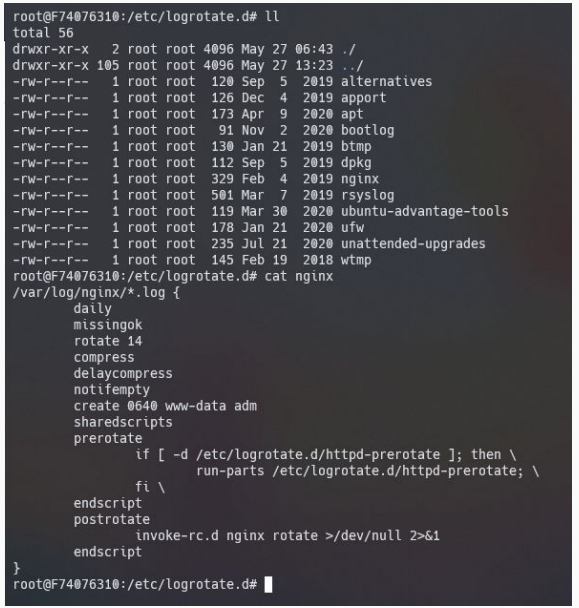
Log files

- For every events in your service / machine
- Purpose
  - Post incident tracking



Logging Policies

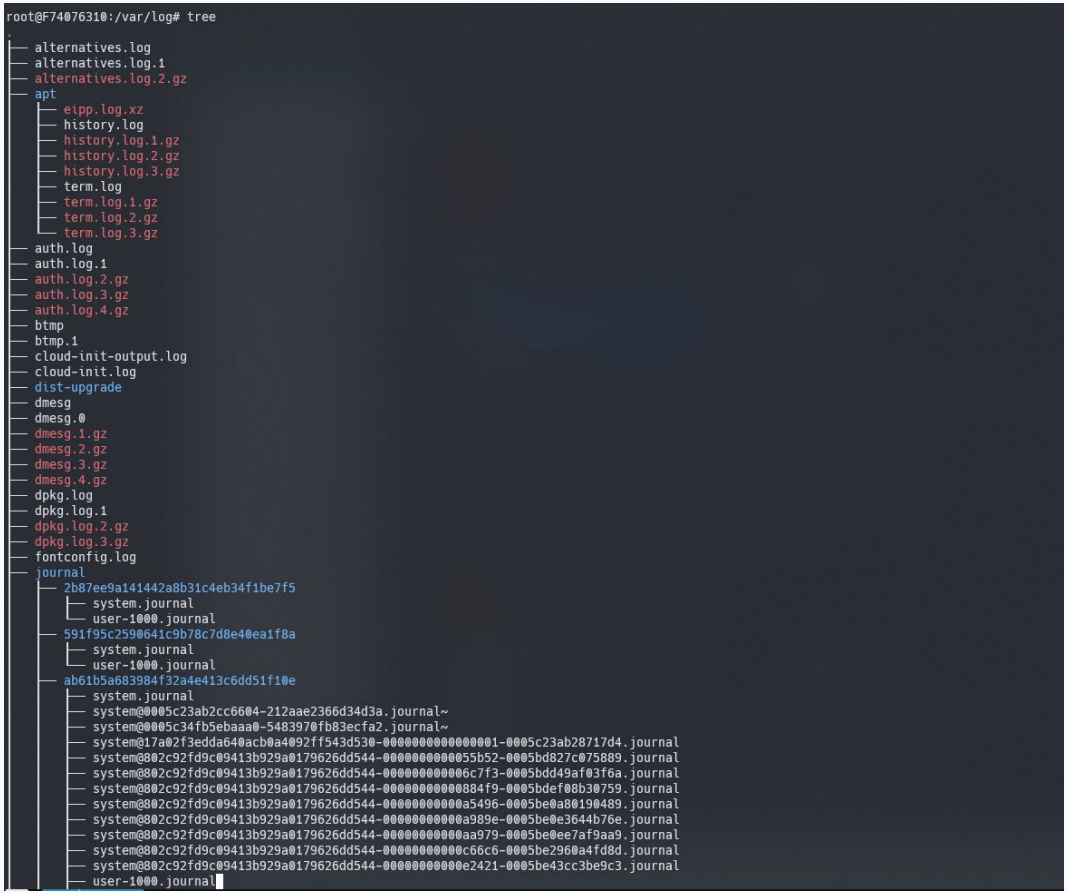
- Throw away all log files
- Rotate log files at periodic intervals
- Archiving log files



Locating Log Files

- Common directory
  - /var/log
- Read software configuration files
  - Ex: nginx
    access_log /var/log/nginx/access.log;
    error_log /var/log/nginx/error.log;
- See /etc/rsyslog.conf

/var/log in Ubuntu Server 20.04



/etc/rsyslog.d/50-default.conf

```
root@F74076310:/var/log# cat /etc/rsyslog.d/50-default.conf
#  Default rules for rsyslog.
#
#                       For more information see rsyslog.conf(5) and /etc/rsyslog.conf

#
# First some standard log files.  Log by facility.
#
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
#daemon.*                       -/var/log/daemon.log
kern.*                          -/var/log/kern.log
#lpr.*                          -/var/log/lpr.log
mail.*                          -/var/log/mail.log
#user.*                         -/var/log/user.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
#mail.info                      -/var/log/mail.info
#mail.warn                      -/var/log/mail.warn
mail.err                        /var/log/mail.err

#
# Some "catch-all" log files.
#
#*.=debug;\
#       auth,authpriv.none;\
#       news.none;mail.none     -/var/log/debug
#*.=info;*.=notice;*.=warn;\
#       auth,authpriv.none;\
#       cron,daemon.none;\
#       mail,news.none          -/var/log/messages

#
# Emergencies are sent to everybody logged in.
#
*.emerg                         :omusrmsg:*

#
# I like to have messages displayed on the console, but only on a virtual
# console I usually leave idle.
#
#daemon,mail.*;\
#       news.=crit;news.=err;news.=notice;\
#       *.=debug;*.=info;\
#       *.=notice;*.=warn       /dev/tty8
root@F74076310:/var/log#
```

Syslog

- Functions
  - Release programmers from writing log files
  - Control of logging
- Parts
  - /etc/rsyslog.conf
  - rsyslogd

/etc/rsyslog.conf

- Basic format
  - selector <TAB> action
    - Selector: program.level
    - Action: What to do
  - Ex:
    - auth,authpriv.* /var/log/auth.log

Configuring syslogd (2/6)

- selector
  - Syntax: facility.level
    - Facility and level are predefined
      (see next page)
  - Combined selector
    - facility.level
    - facility1,facility2.level
    - facility1.level;facility2.level
    - *.level
  - Level indicate the minimum importance that a message must be logged
  - A message matching any selector will be subject to the line's action

Configuring syslogd (3/6)

Facility	Programs that use it
`kern`	The kernel
`user`	User processes (the default if not specified)
`mail`	**sendmail** and other mail-related software
`daemon`	System daemons
`auth`	Security and authorization-related commands
`lpr`	The BSD line printer spooling system
`news`	The Usenet news system
`uucp`	Reserved for UUCP, which doesn't use it
`cron`	The **cron** daemon
`mark`	Timestamps generated at regular intervals
`local0-7`	Eight flavors of local message
`syslog`	**syslogd** internal messages
`authpriv`	Private authorization messages (should all be private, really)
`ftp`	The FTP daemon, **ftpd**
`*`	All facilities except "mark"

Level	Approximate meaning
`emerg`	Panic situations
`alert`	Urgent situations
`crit`	Critical conditions
`err`	Other error conditions
`warning`	Warning messages
`notice`	Things that might merit investigation
`info`	Informational messages
`debug`	For debugging only

facility: auth, authpriv, console, cron, daemon, ftp, kern, lpr, mail, mark, news, ntp, security, syslog, user, uucp, and local0 through local7

Configuring syslogd (4/6)

- Action
  - filename
    - Write the message to a local file
  - @hostname
    - Forward the message to the syslogd on hostname
  - @ipaddress
    - Forwards the message to the host at that IP address
  - user1, user2
    - Write the message to the user's screen if they are logged in
  - *
    - Write the message to all user logged in

```
#  Default rules for rsyslog.
#
#                       For more information see rsyslog.conf(5) and /etc/rsyslog.conf

#
# First some standard log files.  Log by facility.
#
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
#daemon.*                       -/var/log/daemon.log
kern.*                          -/var/log/kern.log
#lpr.*                          -/var/log/lpr.log
mail.*                          -/var/log/mail.log
#user.*                         -/var/log/user.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
#mail.info                      -/var/log/mail.info
#mail.warn                      -/var/log/mail.warn
mail.err                        /var/log/mail.err

#
# Some "catch-all" log files.
#
#*.=debug;\
#       auth,authpriv.none;\
#       news.none;mail.none     -/var/log/debug
#*.=info;*.=notice;*.=warn;\
#       auth,authpriv.none;\
#       cron,daemon.none;\
#       mail,news.none          -/var/log/messages

#
# Emergencies are sent to everybody logged in.
#
*.emerg                         :omusrmsg:*

#
# I like to have messages displayed on the console, but only on a virtual
# console I usually leave idle.
#
#daemon,mail.*;\
#       news.=crit;news.=err;news.=notice;\
#       *.=debug;*.=info;\
#       *.=notice;*.=warn       /dev/tty8
```

Time series Database

Time series Database (TSDB)

- Database optimized for time-stamped or time series data
  - Measurements or events that are tracked, monitored, downsampled, and aggregated over time
- Features
  - INSERT instead of UPDATE
  - Data comes with timestamp
  - Lots of data in a second / minute

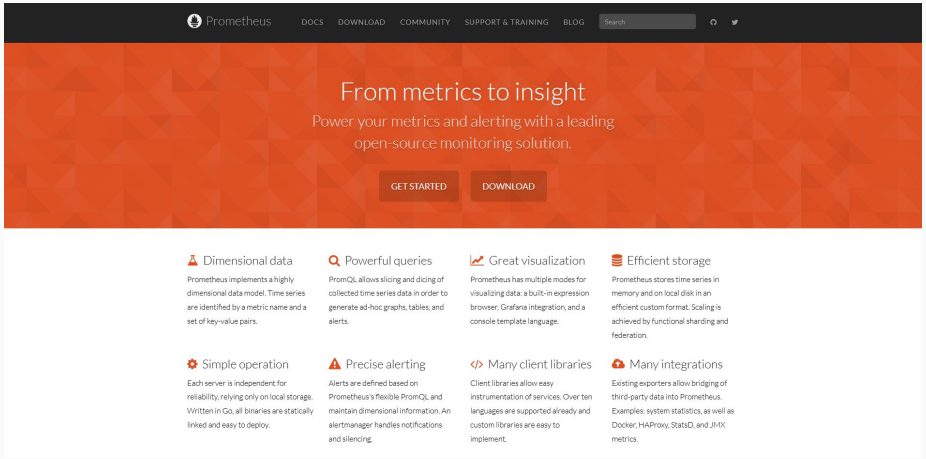
Popular Time series Databases

- Prometheus
- Graphite
- OpenTSDB
- InfluxDB

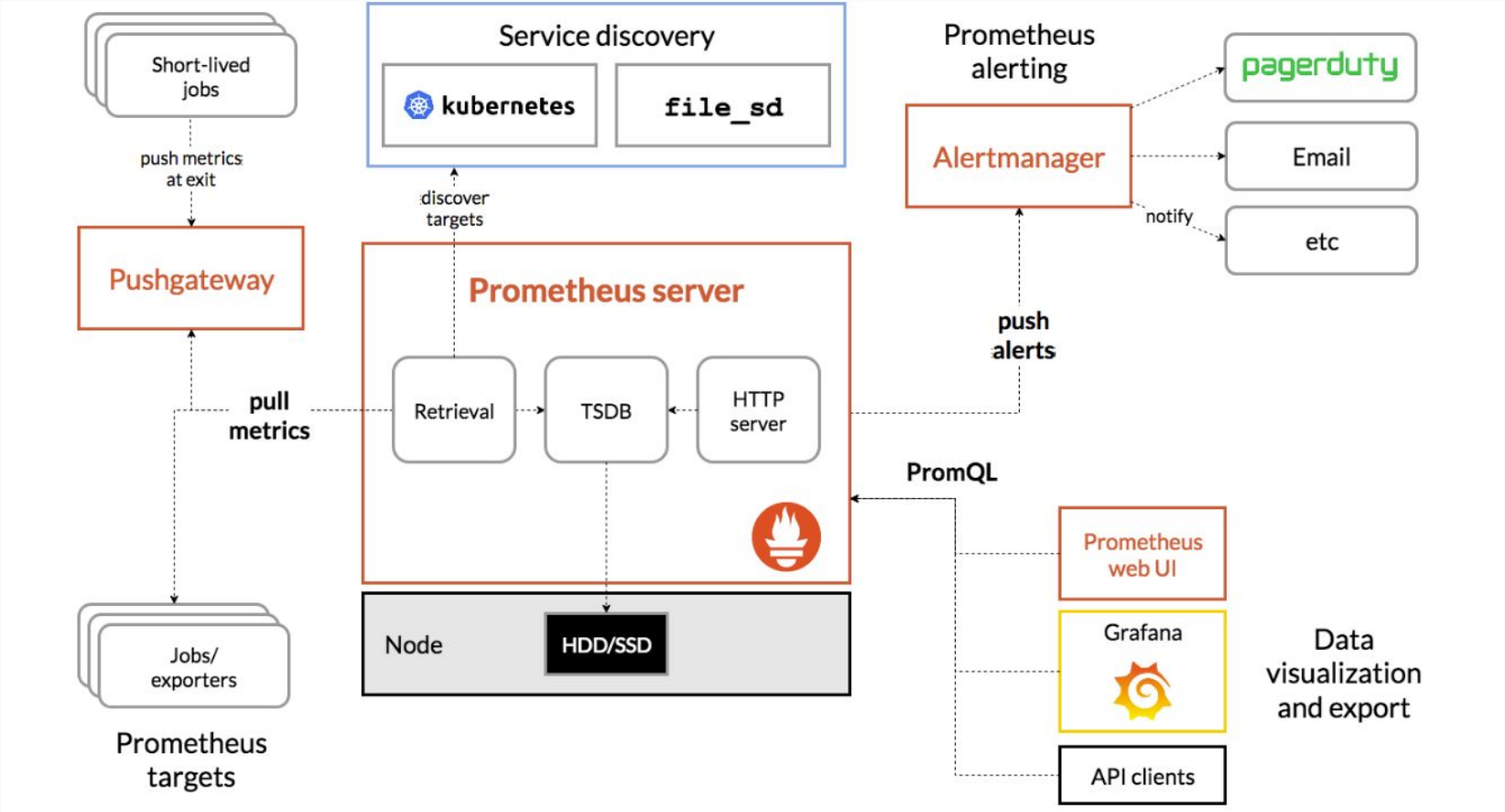
Prometheus

Prometheus

- CNCF graduated project
- Time series collection via pull model over HTTP
- Service Discovery supported
- To be used with
  - *_exporters
  - Pushgateway
  - Alertmanager



Prometheus - Architecture



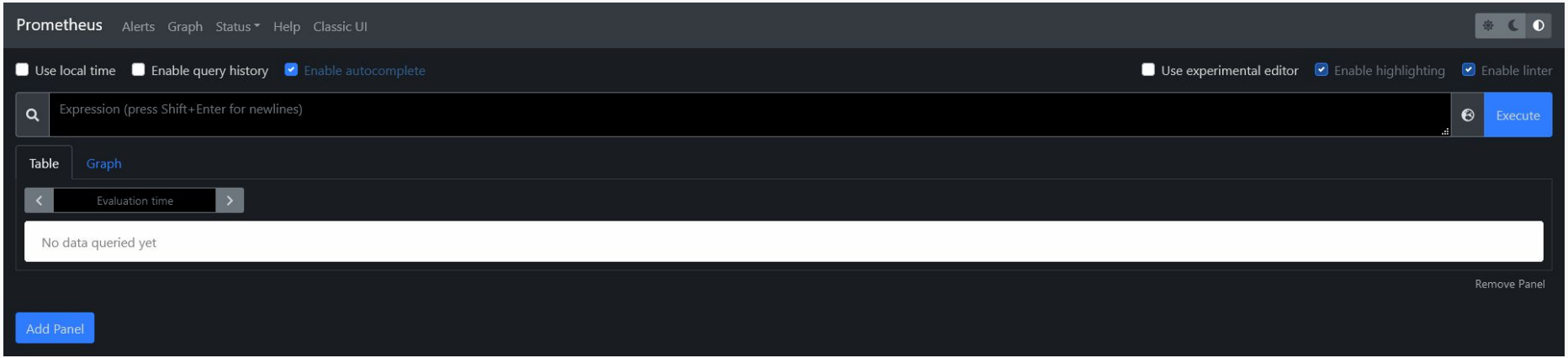
Prometheus - Getting Started

- Grab the latest release
- Configure Prometheus
- Start Prometheus
  - ./prometheus --config.file=prometheus.yml

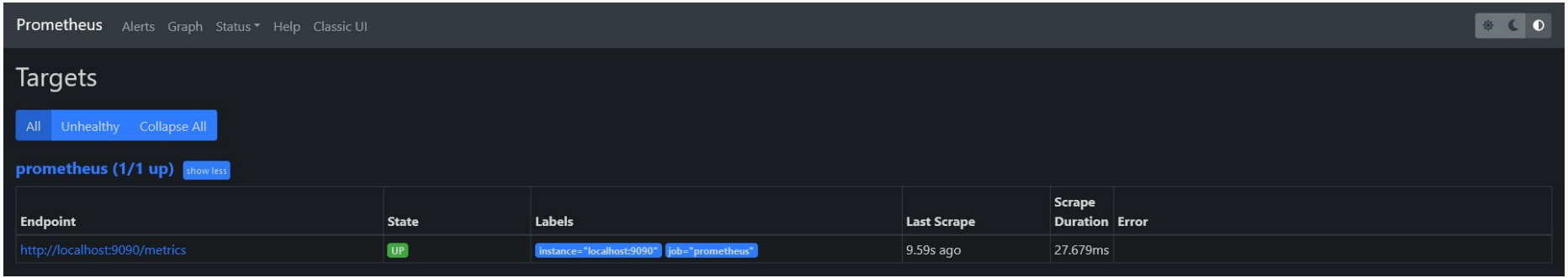
Prometheus - Example Configuration

```
global:
  scrape_interval:     15s # By default, scrape targets every 15 seconds.

  # Attach these labels to any time series or alerts when communicating with
  # external systems (federation, remote storage, Alertmanager).
  external_labels:
    monitor: 'codelab-monitor'

# A scrape configuration containing exactly one endpoint to scrape:
# Here it's Prometheus itself.
scrape_configs:
  # The job name is added as a label `job=<job_name>` to any timeseries scraped from this config.
  - job_name: 'prometheus'

    # Override the global default and scrape targets from this job every 5 seconds.
    scrape_interval: 5s

    static_configs:
      - targets: ['localhost:9090']
```

Prometheus - Graph Page



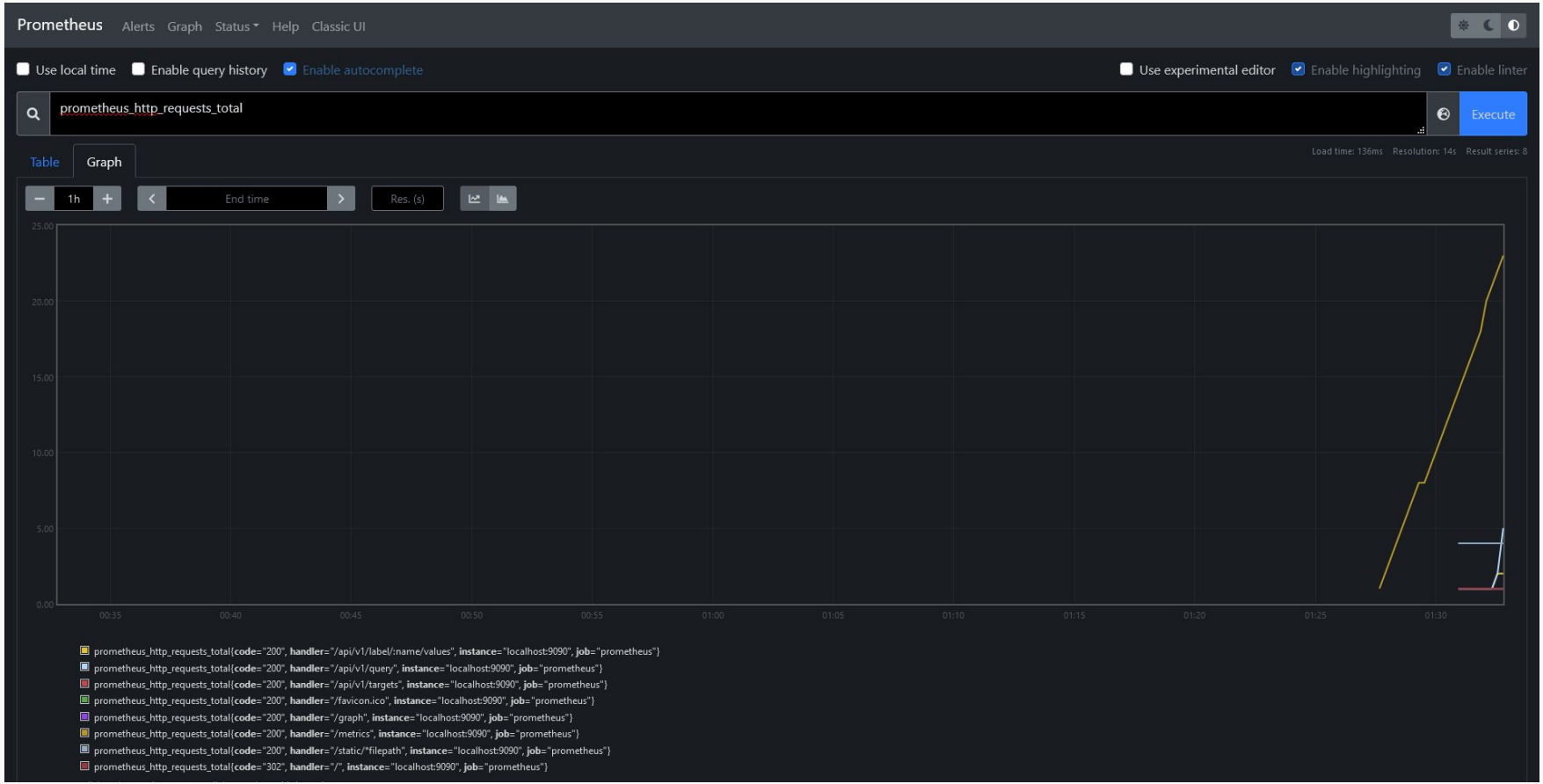
Prometheus - Targets



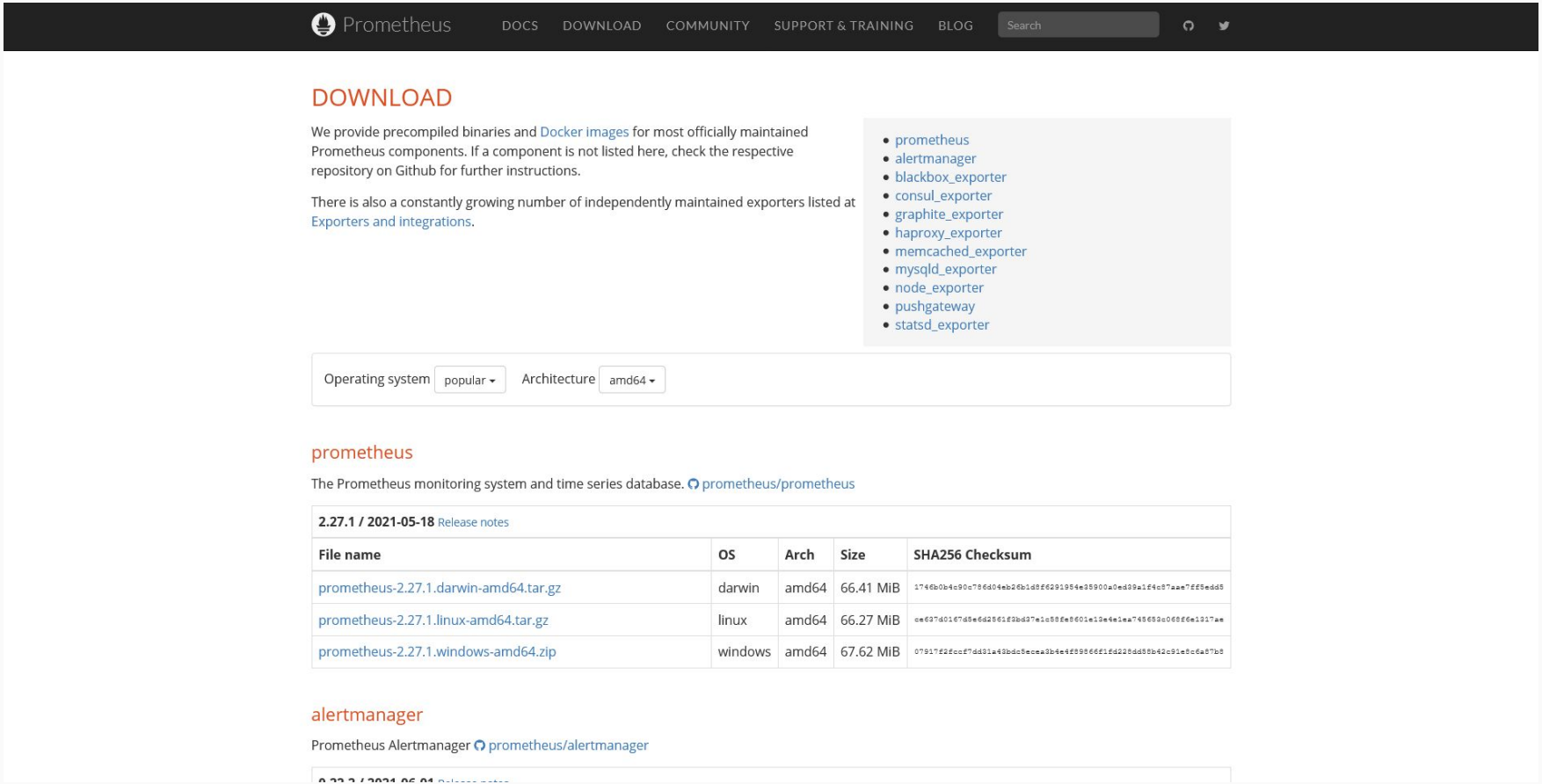
Prometheus - Server Metrics

```
# HELP go_gc_duration_seconds A summary of the pause duration of garbage collection cycles.
# TYPE go_gc_duration_seconds summary
go_gc_duration_seconds{quantile="0"} 4.0842e-05
go_gc_duration_seconds{quantile="0.25"} 4.2288e-05
go_gc_duration_seconds{quantile="0.5"} 6.5854e-05
go_gc_duration_seconds{quantile="0.75"} 0.001084194
go_gc_duration_seconds{quantile="1"} 0.00130079
go_gc_duration_seconds_sum 0.002674114
go_gc_duration_seconds_count 7
# HELP go_goroutines Number of goroutines that currently exist.
# TYPE go_goroutines gauge
go_goroutines 34
# HELP go_info Information about the Go environment.
# TYPE go_info gauge
go_info{version="go1.16.4"} 1
# HELP go_memstats_alloc_bytes Number of bytes allocated and still in use.
# TYPE go_memstats_alloc_bytes gauge
go_memstats_alloc_bytes 1.634368e+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 2.9477704e+07
# 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 1.45428e+06
# HELP go_memstats_frees_total Total number of frees.
# TYPE go_memstats_frees_total counter
go_memstats_frees_total 117431
# HELP go_memstats_gc_cpu_fraction The fraction of this program's available CPU time used by the GC since the program started.
# TYPE go_memstats_gc_cpu_fraction gauge
go_memstats_gc_cpu_fraction 0.0002395509032689669
# HELP go_memstats_gc_sys_bytes Number of bytes used for garbage collection system metadata.
# TYPE go_memstats_gc_sys_bytes gauge
go_memstats_gc_sys_bytes 5.848832e+06
# HELP go_memstats_heap_alloc_bytes Number of heap bytes allocated and still in use.
# TYPE go_memstats_heap_alloc_bytes gauge
go_memstats_heap_alloc_bytes 1.634368e+07
# HELP go_memstats_heap_idle_bytes Number of heap bytes waiting to be used.
# TYPE go_memstats_heap_idle_bytes gauge
go_memstats_heap_idle_bytes 4.7980544e+07
# HELP go_memstats_heap_inuse_bytes Number of heap bytes that are in use.
# TYPE go_memstats_heap_inuse_bytes gauge
go_memstats_heap_inuse_bytes 1.847296e+07
# HELP go_memstats_heap_objects Number of allocated objects.
# TYPE go_memstats_heap_objects gauge
go_memstats_heap_objects 85342
# HELP go_memstats_heap_released_bytes Number of heap bytes released to OS.
# TYPE go_memstats_heap_released_bytes gauge
go_memstats_heap_released_bytes 4.5416448e+07
# HELP go_memstats_heap_sys_bytes Number of heap bytes obtained from system.
# TYPE go_memstats_heap_sys_bytes gauge
go_memstats_heap_sys_bytes 6.6453504e+07
# HELP go_memstats_last_gc_time_seconds Number of seconds since 1970 of last garbage collection.
# TYPE go_memstats_last_gc_time_seconds gauge
go_memstats_last_gc_time_seconds 1.622683862701196e+09
# HELP go_memstats_lookups_total Total number of pointer lookups.
# TYPE go_memstats_lookups_total counter
go_memstats_lookups_total 0
# HELP go_memstats_mallocs_total Total number of mallocs.
# TYPE go_memstats_mallocs_total counter
go_memstats_mallocs_total 202773
# HELP go_memstats_mcache_inuse_bytes Number of bytes in use by mcache structures.
# TYPE go_memstats_mcache_inuse_bytes gauge
go_memstats_mcache_inuse_bytes 1200
# HELP go_memstats_mcache_sys_bytes Number of bytes used for mcache structures obtained from system.
```

Prometheus - Graph Example



Prometheus - Official Exporter



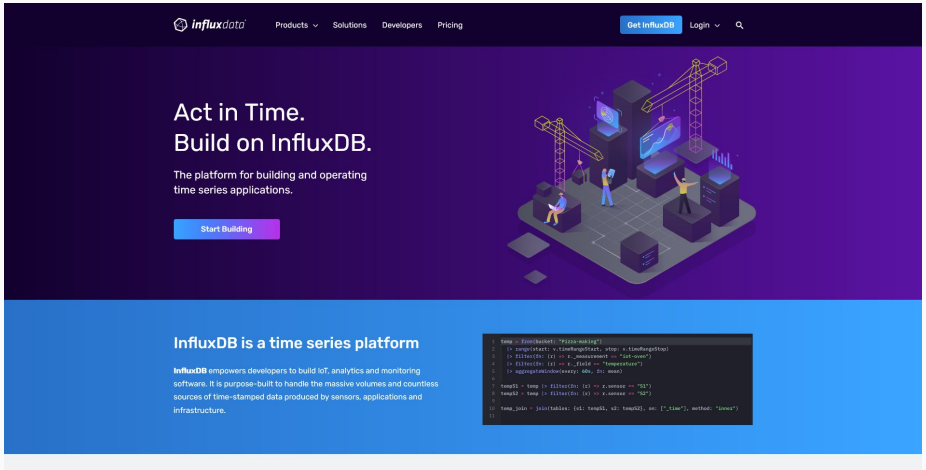
Prometheus - Monitor Multiple Endpoints

```
scrape_configs:
  - job_name:       'node'

    # Override the global default and scrape targets from this job every 5 seconds.
    scrape_interval: 5s

    static_configs:
      - targets: ['localhost:8080', 'localhost:8081']
        labels:
          group: 'production'

      - targets: ['localhost:8082']
        labels:
          group: 'canary'
```

InfluxDB

InfluxData

- Company behind InfluxDB
- Products
  - InfluxDB
    - 1.x
    - 2.0 (Mainline)
  - Telegraf

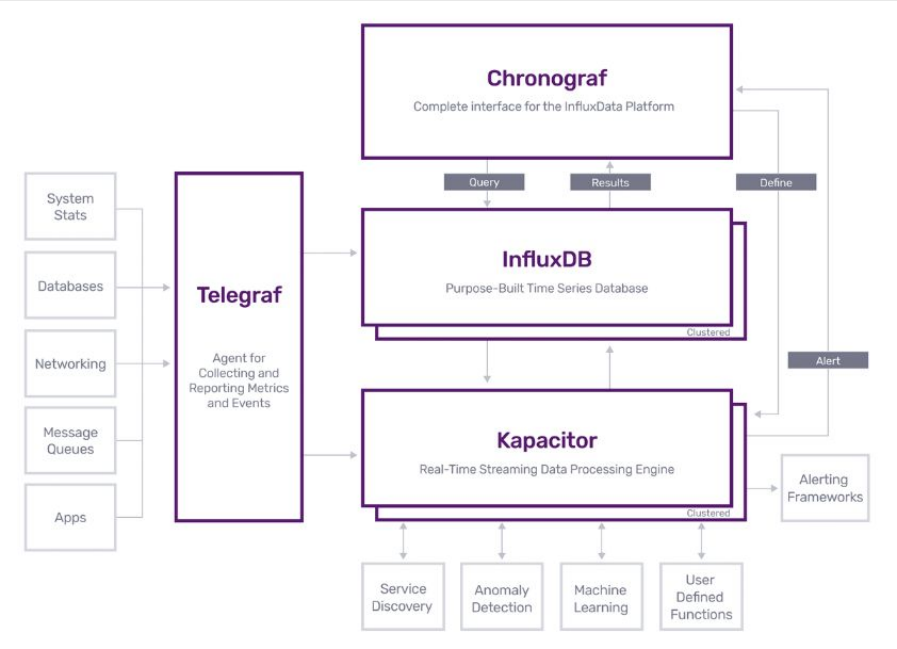


InfluxDB

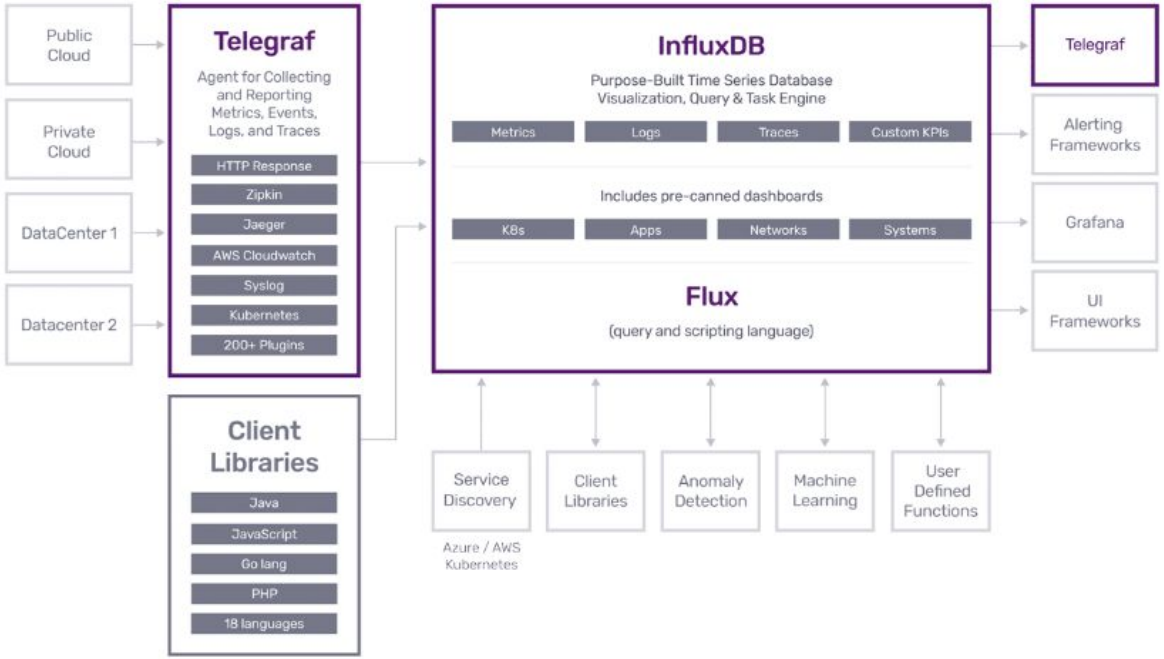
- Push over HTTP model
- Built-in Visualizer
- Built-in Dashboard
- Built-in Alert System

InfluxDB 1.x - TICK Stack

- Telegraf
- InfluxDB
- Chronograf
- Kapacitor



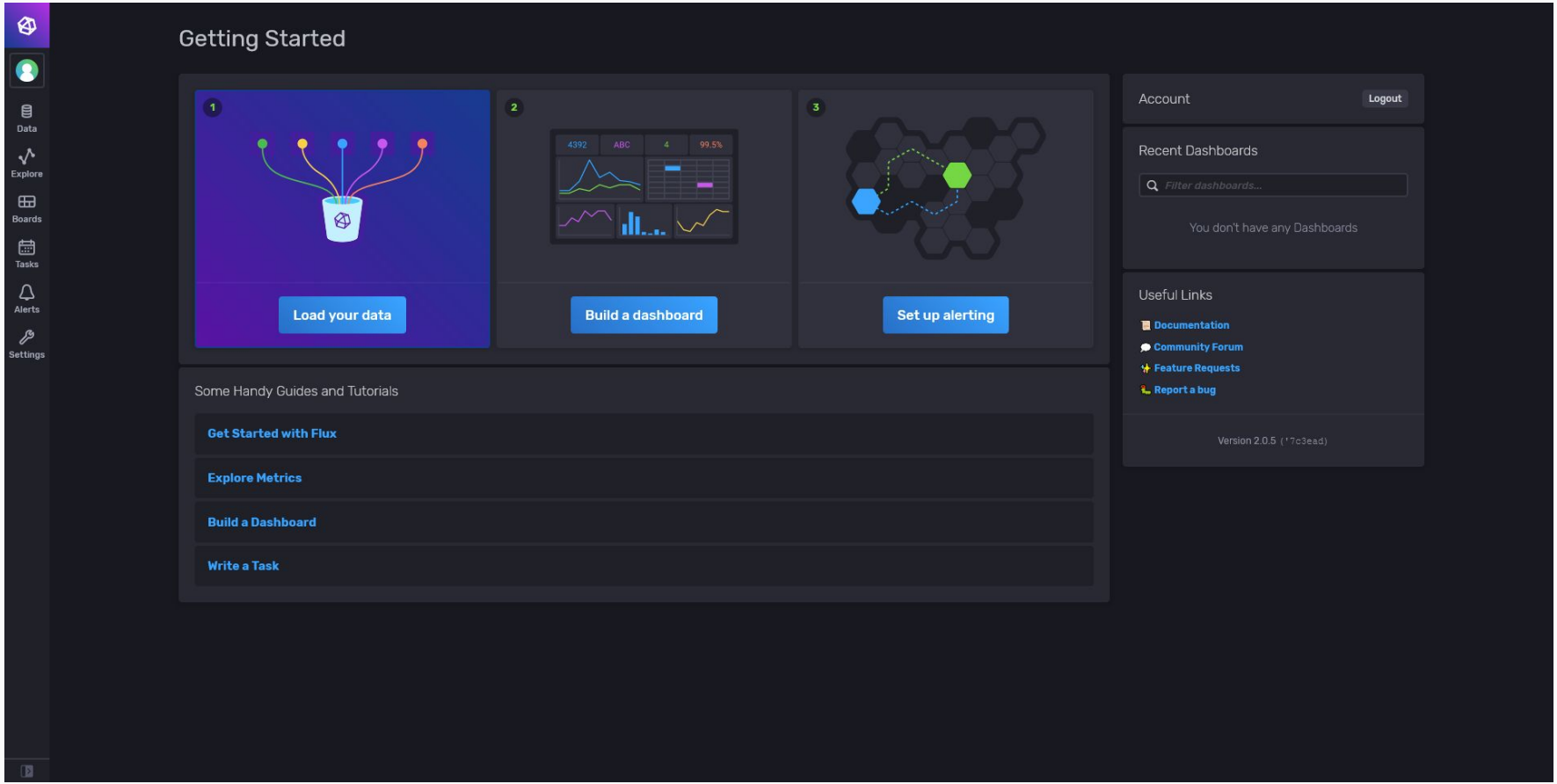
InfluxDB 2.0 - InfluxDB & Telegraf



InfluxDB 2.0 - Getting Started

- Install InfluxDB 2.0
- Basic setup
- Install Telegraf

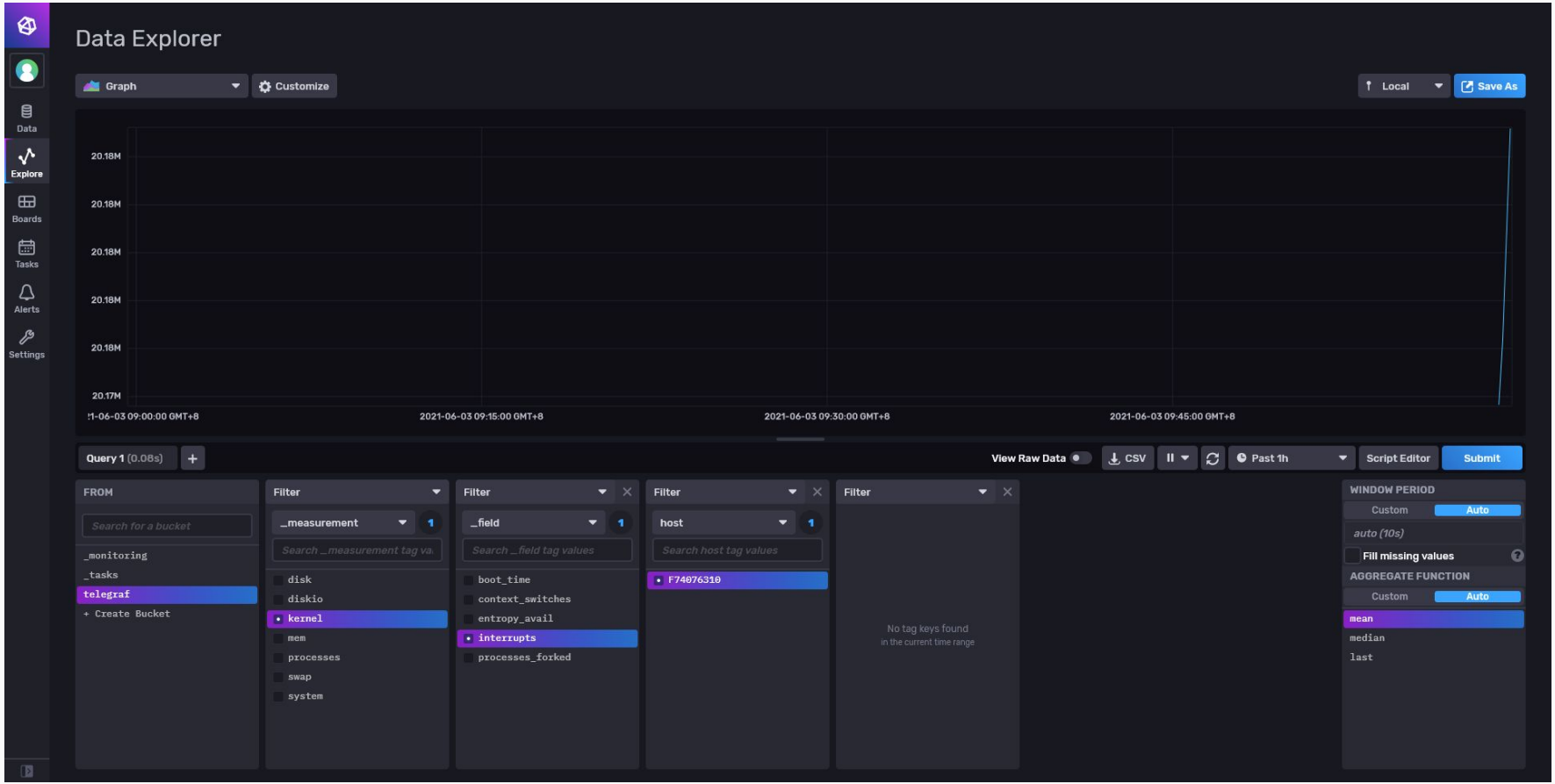
InfluxDB 2.0 - Homepage



Telegraf - InfluxDB 2.0 Output

```
# # Configuration for sending metrics to InfluxDB
# [[outputs.influxdb_v2]]
#   ## The URLs of the InfluxDB cluster nodes.
#   ##
#   ## Multiple URLs can be specified for a single cluster, only ONE of the
#   ## urls will be written to each interval.
#   ##   ex: urls = ["https://us-west-2-1.aws.cloud2.influxdata.com"]
#   urls = ["http://127.0.0.1:8086"]
#
#   ## Token for authentication.
#   token = ""
#
#   ## Organization is the name of the organization you wish to write to; must exist.
#   organization = ""
#
#   ## Destination bucket to write into.
#   bucket = ""
#
#   ## The value of this tag will be used to determine the bucket.  If this
#   ## tag is not set the 'bucket' option is used as the default.
#   # bucket_tag = ""
#
#   ## If true, the bucket tag will not be added to the metric.
#   # exclude_bucket_tag = false
#
#   ## Timeout for HTTP messages.
#   # timeout = "5s"
#
#   ## Additional HTTP headers
#   # http_headers = {"X-Special-Header" = "Special-Value"}
#
#   ## HTTP Proxy override, if unset values the standard proxy environment
#   ## variables are consulted to determine which proxy, if any, should be used.
#   # http_proxy = "http://corporate.proxy:3128"
#
#   ## HTTP User-Agent
#   # user_agent = "telegraf"
#
#   ## Content-Encoding for write request body, can be set to "gzip" to
#   ## compress body or "identity" to apply no encoding.
#   # content_encoding = "gzip"
#
#   ## Enable or disable uint support for writing uints influxdb 2.0.
#   # influx_uint_support = false
#
#   ## Optional TLS Config for use on HTTP connections.
#   # tls_ca = "/etc/telegraf/ca.pem"
#   # tls_cert = "/etc/telegraf/cert.pem"
#   # tls_key = "/etc/telegraf/key.pem"
#   ## Use TLS but skip chain & host verification
#   # insecure_skip_verify = false
```

InfluxDB - Data Explorer



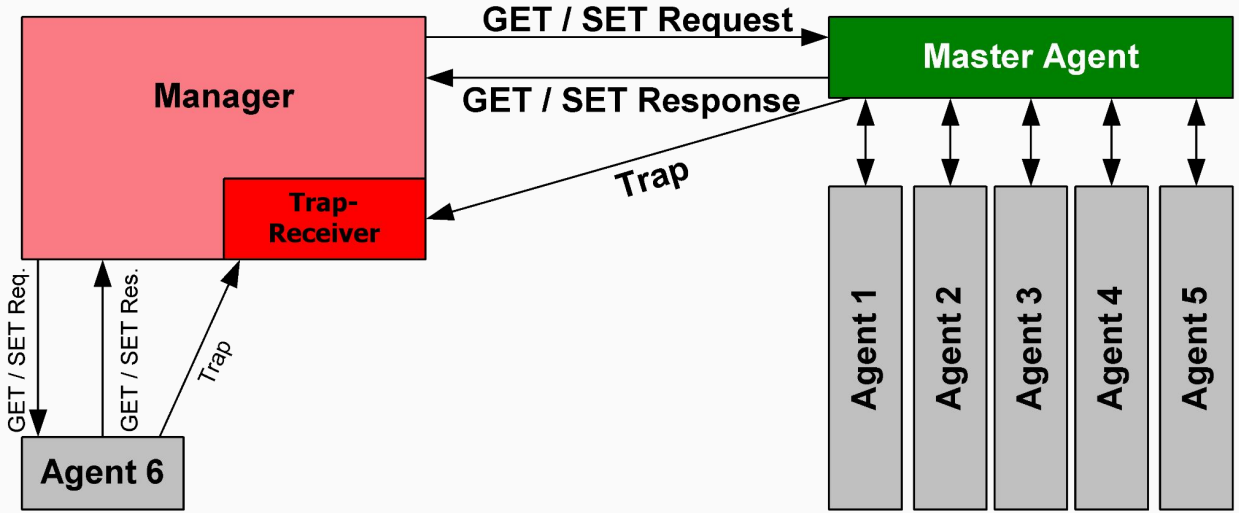
SNMP

SNMP

- Simple Network Management Protocol
- L7 protocol
- composed by 3 part
  - NMSs, Network-management systems
  - managed device
  - agent

SNMP - Workflow

- install agent on device you want to manage



Install agent

- apt update; apt install snmpd snmp
- vim /etc/snmp/snmpd.conf
  - add “ro community public 127.0.0.1”
  - this mean add read only permission to 127.0.0.1
- systemctl enable snmpd --now
- snmpwalk -v 2c 127.0.0.1 -c public [OID]
  - show snmp data
  - -v: snmp version(we choose 2c in this class, it’s much easier)
  - [OID]: object id(empty will print all data)

It’s hard to read

OID

```
F74061030@F74061030 ~ snmpwalk -v 2c 127.0.0.1 -c public .1.3.6.1.4.1.2021.4
iso.3.6.1.4.1.2021.4.1.0 = INTEGER: 0
iso.3.6.1.4.1.2021.4.2.0 = STRING: "swap"
iso.3.6.1.4.1.2021.4.3.0 = INTEGER: 0
iso.3.6.1.4.1.2021.4.4.0 = INTEGER: 0
iso.3.6.1.4.1.2021.4.5.0 = INTEGER: 1004720
iso.3.6.1.4.1.2021.4.6.0 = INTEGER: 164552
iso.3.6.1.4.1.2021.4.11.0 = INTEGER: 164552
iso.3.6.1.4.1.2021.4.12.0 = INTEGER: 16000
iso.3.6.1.4.1.2021.4.13.0 = INTEGER: 3444
iso.3.6.1.4.1.2021.4.14.0 = INTEGER: 93088
iso.3.6.1.4.1.2021.4.15.0 = INTEGER: 471328
iso.3.6.1.4.1.2021.4.18.0 = Counter64: 0
iso.3.6.1.4.1.2021.4.19.0 = Counter64: 0
iso.3.6.1.4.1.2021.4.20.0 = Counter64: 1004720
iso.3.6.1.4.1.2021.4.21.0 = Counter64: 164552
iso.3.6.1.4.1.2021.4.22.0 = Counter64: 164552
iso.3.6.1.4.1.2021.4.23.0 = Counter64: 16000
iso.3.6.1.4.1.2021.4.24.0 = Counter64: 3444
iso.3.6.1.4.1.2021.4.25.0 = Counter64: 93088
iso.3.6.1.4.1.2021.4.26.0 = Counter64: 471328
iso.3.6.1.4.1.2021.4.100.0 = INTEGER: 1
iso.3.6.1.4.1.2021.4.101.0 = STRING: "Running out of swap space (0)"
```

- vim /etc/snmp/snmp.conf
  - # mib: <- comment this line

Much better

better OID

```
F74061030@F74061030 ~ snmpwalk -v 2c 127.0.0.1 -c public .1.3.6.1.4.1.2021.4
UCD-SNMP-MIB::memIndex.0 = INTEGER: 0
UCD-SNMP-MIB::memErrorName.0 = STRING: swap
UCD-SNMP-MIB::memTotalSwap.0 = INTEGER: 0 kB
UCD-SNMP-MIB::memAvailSwap.0 = INTEGER: 0 kB
UCD-SNMP-MIB::memTotalReal.0 = INTEGER: 1004720 kB
UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 164048 kB
UCD-SNMP-MIB::memTotalFree.0 = INTEGER: 164048 kB
UCD-SNMP-MIB::memMinimumSwap.0 = INTEGER: 16000 kB
UCD-SNMP-MIB::memShared.0 = INTEGER: 3444 kB
UCD-SNMP-MIB::memBuffer.0 = INTEGER: 93140 kB
UCD-SNMP-MIB::memCached.0 = INTEGER: 471328 kB
UCD-SNMP-MIB::memTotalSwapX.0 = Counter64: 0 kB
UCD-SNMP-MIB::memAvailSwapX.0 = Counter64: 0 kB
UCD-SNMP-MIB::memTotalRealX.0 = Counter64: 1004720 kB
UCD-SNMP-MIB::memAvailRealX.0 = Counter64: 164048 kB
UCD-SNMP-MIB::memTotalFreeX.0 = Counter64: 164048 kB
UCD-SNMP-MIB::memMinimumSwapX.0 = Counter64: 16000 kB
UCD-SNMP-MIB::memSharedX.0 = Counter64: 3444 kB
UCD-SNMP-MIB::memBufferX.0 = Counter64: 93140 kB
UCD-SNMP-MIB::memCachedX.0 = Counter64: 471328 kB
UCD-SNMP-MIB::memSwapError.0 = INTEGER: error(1)
```

https://www.manageengine.com/tw/network-monitoring/what-is-snmp.html

管理資訊資料庫或管理資訊庫 (MIB)

每個 SNMP 代理程式都有一個描述受控裝置參數資訊資料庫。SNMP 管理器使用此資料庫，向代理程式請求特定資訊，並根據網路管理系統 (NMS) 的需求，進一步翻譯資訊。代理程式和管理器之間共用的資料庫稱為管理資訊庫 (MIB)。

通常，這些 MIB 包含為網路上的硬體節點定義的標準統計和控制值集合。SNMP 還允許透過使用私人 MIB ，將特定於特定代理程式的值，擴展到這些標準值。

簡而言之，MIB 檔案是 SNMP 管理器可以詢問代理程式的問題集合。如 MIB 中所定義，代理程式在本地收集這些資料並將其存儲。因此，SNMP 管理器應該了解每種類型代理程式的這些標準和私人問題。

MIB can map object ID to device

MIB 結構和物件識別碼（物件 ID 或 OID）

管理資訊庫 (MIB) 是用於管理網路元素的資訊的集合。MIB 包含由名稱物件識別碼（物件 ID 或 OID）標識的受控物件。

每個識別碼都是唯一的，並表示受控裝置的特定特性。當查詢時，每個識別碼的返回值可能不同，如文字、數字、計數等...

有兩種類型的受控物件或物件 ID：純量和表格式。透過一個例子來更好的理解它們

純量：裝置的廠商名稱，結果只能有一個。（如定義所述：「純量物件定義單個物件執行個體」）

表格式：四元組處理器的 CPU 使用率，這將分別為每個 CPU 給出結果，這意味著該特定物件 ID 將有 4 個結果。（如定義所述：「表格式物件定義了在 MIB 表格中分組在一起的多個相關物件執行個體」）

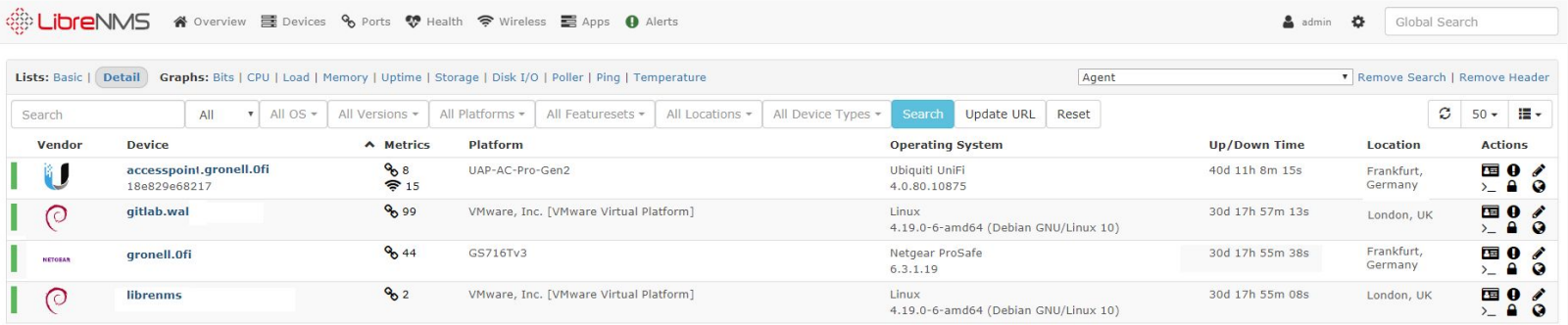
每個物件 ID 都是在 MIB 中按階層組織的。MIB 階層可以用具有單個變數識別碼的樹狀結構表示。

一個典型物件 ID 將是一個整數的點線清單。例如，RFC1213 中「sysDescr」的 OID 為 .1.3.6.1.2.1.1.1

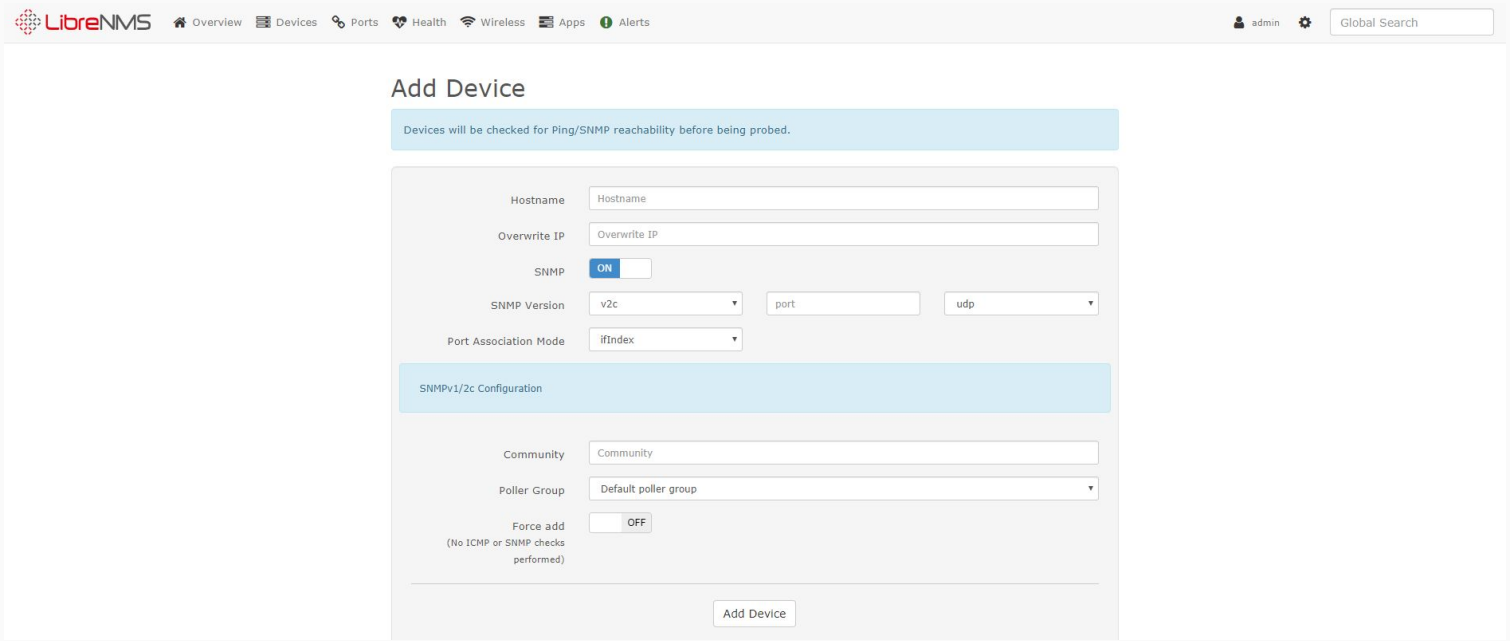
LibreNMS

- Automatically discover your entire network using CDP, FDP, LLDP, OSPF, BGP, SNMP and ARP.
- Highly flexible alerting system, notify via email, irc, slack and more.
- A full API to manage, graph and retrieve data from your install.

LibreNMS


LibreNMS
Overview
Devices
Ports
Health
Wireless
Apps
Alerts
admin
Global Search
Lists: Basic | Detail Graphs: Bits | CPU | Load | Memory | Uptime | Storage | Disk I/O | Poller | Ping | Temperature
Agent
Remove Search | Remove Header
Search
All
All OS
All Versions
All Platforms
All Featuresets
All Locations
All Device Types
Search
Update URL
Reset
50
Vendor
Device
Metrics
Platform
Operating System
Up/Down Time
Location
Actions
accesspoint.gronell.0fi
18e829e68217
8
15
UAP-AC-Pro-Gen2
Ubiquiti UniFi
4.0.80.10875
40d 11h 8m 15s
Frankfurt, Germany
gitlab.wal
99
VMware, Inc. [VMware Virtual Platform]
Linux
4.19.0-6-amd64 (Debian GNU/Linux 10)
30d 17h 57m 13s
London, UK
gronell.0fi
44
GS716Tv3
Netgear ProSafe
6.3.1.19
30d 17h 55m 38s
Frankfurt, Germany
librenms
2
VMware, Inc. [VMware Virtual Platform]
Linux
4.19.0-6-amd64 (Debian GNU/Linux 10)
30d 17h 55m 08s
London, UK

LibreNMS


LibreNMS
Overview
Devices
Ports
Health
Wireless
Apps
Alerts
admin
Global Search
Add Device
Devices will be checked for Ping/SNMP reachability before being probed.
Hostname
Hostname
Overwrite IP
Overwrite IP
SNMP
ON
SNMP Version
v2c
port
udp
Port Association Mode
ifIndex
SNMPv1/2c Configuration
Community
Community
Poller Group
Default poller group
Force add
(No ICMP or SNMP checks performed)
OFF
Add Device

LibreNMS


LibreNMS
Overview
Devices
Ports
Health
Wireless
Apps
Alerts
admin
Global Search
Ports lists » Basic | Detail Graphs » Bits | Unicast Packets | Non-Unicast Packets | Errors
Export CSV | Update URL | Search | Header | Bulk actions » Purge all deleted
gronell.Ofi::eth0
gronell.Ofi::lo
librenms::venet0
librenms::lo
server-test::lo
server-test::venet0
shizuku.srv::eth0
shizuku.srv::lo
Fri 00:00
Fri 12:00

Grafana

Grafana

- Fashion visualize tool
- Support a lot data source
  - AWS CloudWatch
  - Azure Monitor
  - Elasticsearch
  - Google Cloud Monitoring
  - InfluxDB
  - Prometheus
  - ...

It’s so hard

- if you want your dashboard as fashion as that video example
  - Working hard
  - Hiring a part time student with 160 NTD/hr ✓

Don’t reinventing the wheel

- Just download & edit dashboards on https://grafana.com/grafana/dashboards
  - ~~But still hire a part time student with 160 NTD/hr~~ ✓

Log Aggregator

Sending Log

- Syslog Server
- Program built-in function
- Log collector

Log collector

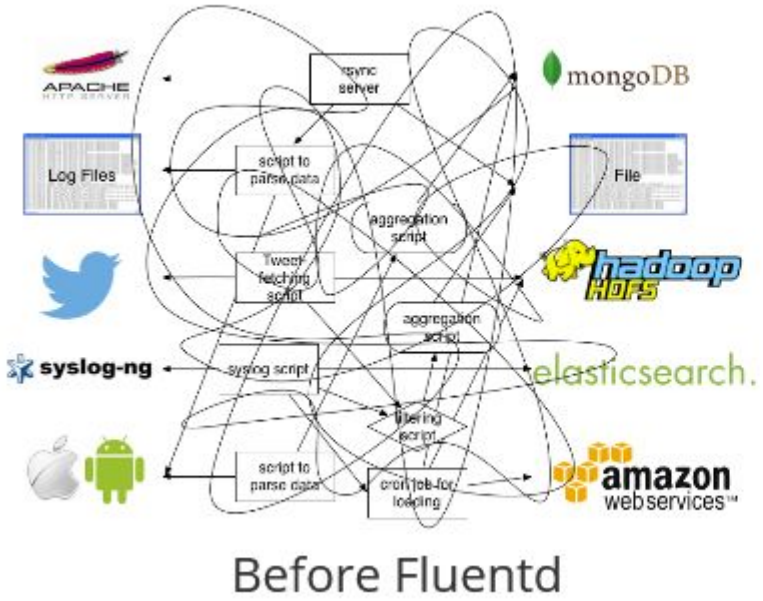
- FluentD
- Splunk
- Telegraf
- Elastic Beats

Fluentd

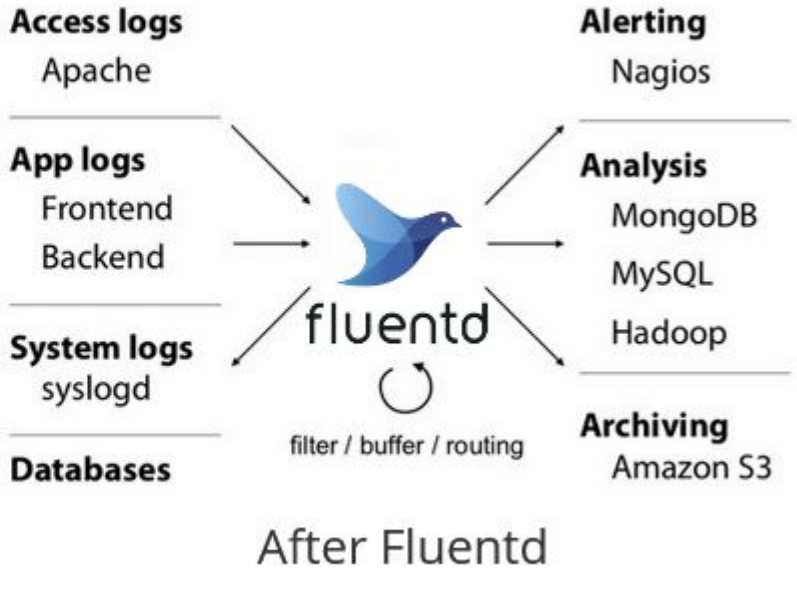
Fluentd

- CNCF member project
- Unified Logging with JSON
- Pluggable Architecture
- Minimum Resources Required
- Built-in Reliability

Why Fluentd?



Before Fluentd



After Fluentd

Fluentd - Get Started

- Install by DEB Package (Debian/Ubuntu)
- Configure
  - Source
  - Match
  - Filter

Fluentd - Configuration - Source

```
# Receive events from 24224/tcp
# This is used by log forwarding and the fluent-cat command
<source>
  @type forward
  port 24224
</source>

# http://<ip>:9880/myapp.access?json={"event":"data"}
<source>
  @type http
  port 9880
</source>
```

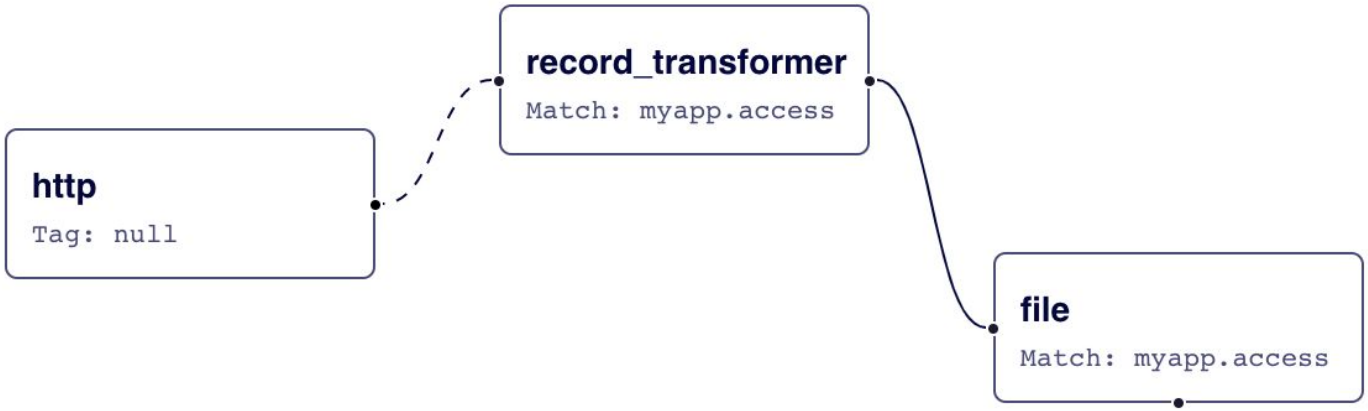
Fluentd - Configuration - Match

```
# Receive events from 24224/tcp
# This is used by log forwarding and the fluent-cat command
<source>
  @type forward
  port 24224
</source>

# http://<ip>:9880/myapp.access?json={"event":"data"}
<source>
  @type http
  port 9880
</source>

# Match events tagged with "myapp.access" and
# store them to /var/log/fluent/access.%Y-%m-%d
# Of course, you can control how you partition your data
# with the time_slice_format option.
<match myapp.access>
  @type file
  path /var/log/fluent/access
</match>
```

Fluentd - Configuration - Filter

```
# http://this.host:9880/myapp.access?json={"event":"data"}
<source>
  @type http
  port 9880
</source>

<filter myapp.access>
  @type record_transformer
  <record>
    host_param "#{Socket.gethostname}"
  </record>
</filter>

<match myapp.access>
  @type file
  path /var/log/fluent/access
</match>
```

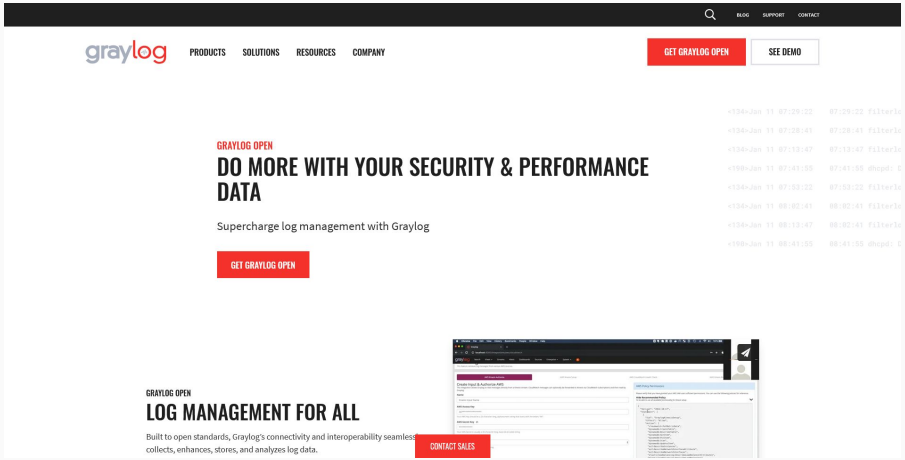
Fluentd - Configuration - Event Route



Graylog

Graylog

- Log Management Software
- Dashboards
- Search
- Fault Tolerance
- Content Packs
- Graylog Sidecar



Graylog - Getting Started

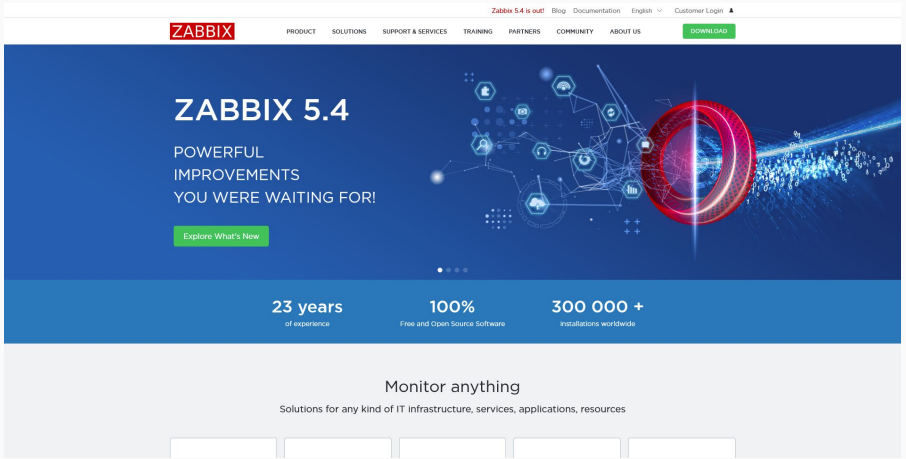
...not going to due that, due to limited resources for VM

Sadly, Graylog removed their demo site

Network Monitoring

Zabbix

- Support Pull & Push Model
- Good for network equipment monitoring
- Scalability / Distributed Monitoring / HA / Security



Zabbix technical demo video

Zabbix 5.4 is out! Blog Documentation English Customer Login

ZABBIX PRODUCT SOLUTIONS SUPPORT & SERVICES TRAINING PARTNERS COMMUNITY ABOUT US DOWNLOAD

Home / Product /

Zabbix technical demo video

Explore quick technical overview of Zabbix features.

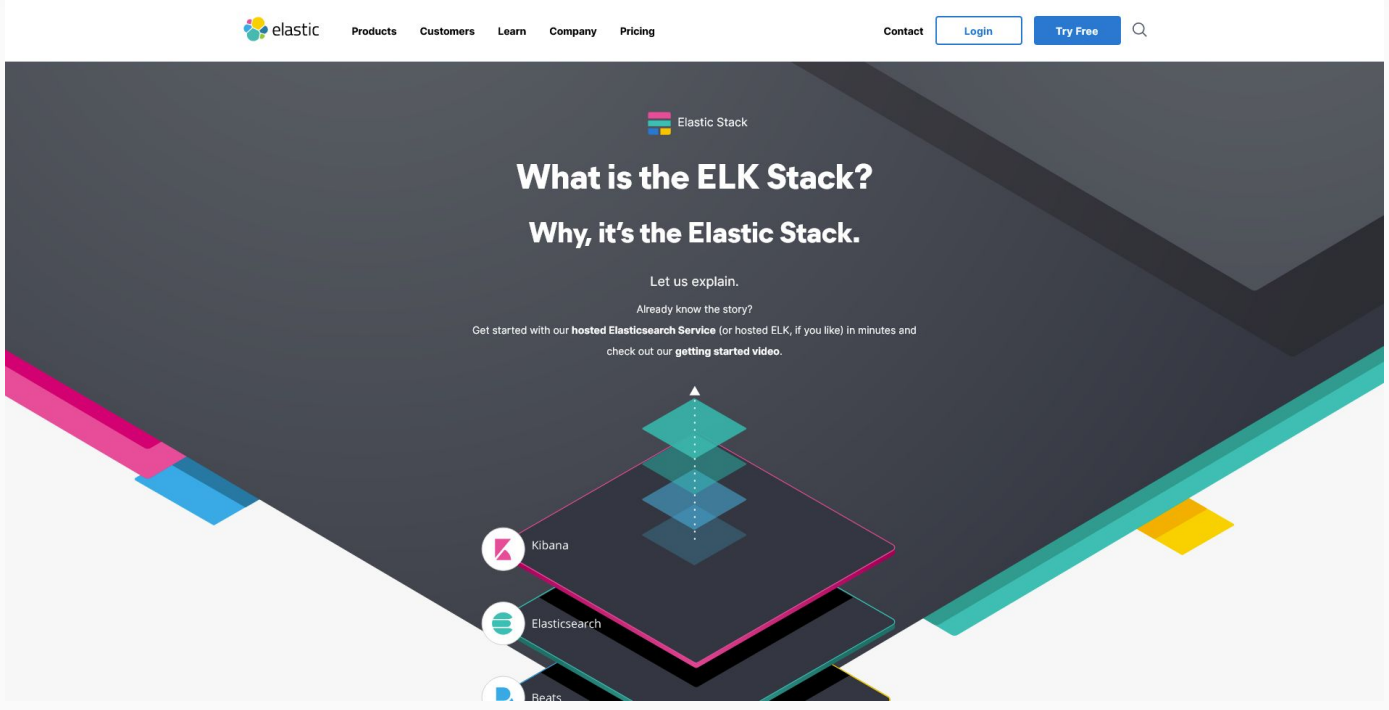
Transcription

Zabbix is an enterprise-level open-source monitoring tool, which has been named the Gartner Customers' Choice for two years in a row. We are sure that this demo video will help you better understand our monitoring solution and get an overview of its core features and functionalities. We will introduce you to both the UI and the basic concepts of monitoring with Zabbix. We hope you will enjoy this brief overview. Welcome to monitoring with Zabbix!

Dashboards

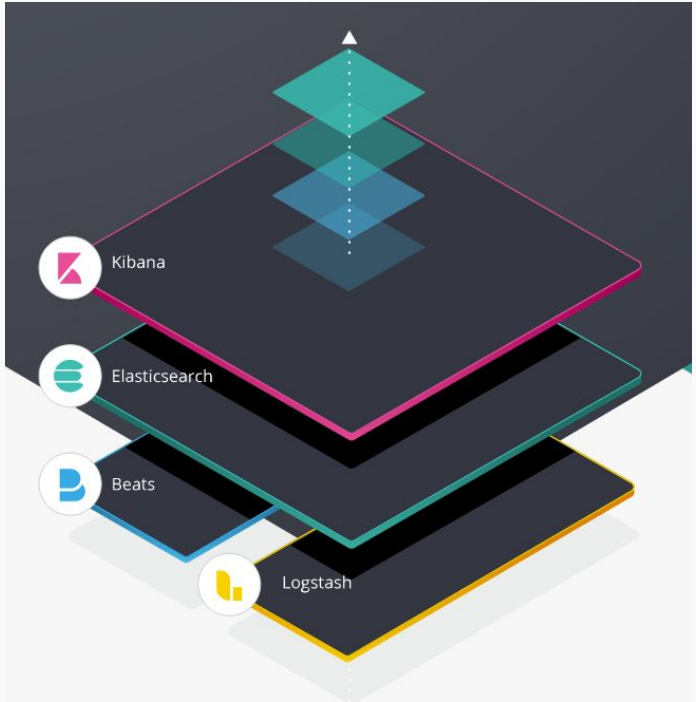
Monitoring Suite

ELK Stack - Elasticsearch / Logstash / Kibana



Elastic Products

- Kibana
- Elasticsearch
- Beats
- Logstash



Kibana

- User interface to visualize Elasticsearch data
- Support various data sources
- Support Pipelines
- Support User / Role

Elasticsearch

- Based on Apache Lucene
- Distributed, RESTful search and analytics engine
- Near real-time search
- Split index into shards so it can be distributed onto different nodes

Logstash

- Input data from various sources
- Parse & Transform data
- Send data to database for long term storage

Beats

- Module installed on every node to export data to Elasticsearch
- Lots of modules
  - Filebeat
  - Metricbeat
  - Packetbeat
  - Winlogbeat
  - Auditbeat
  - Heartbeat
  - Functionbeat
  - ...lots more

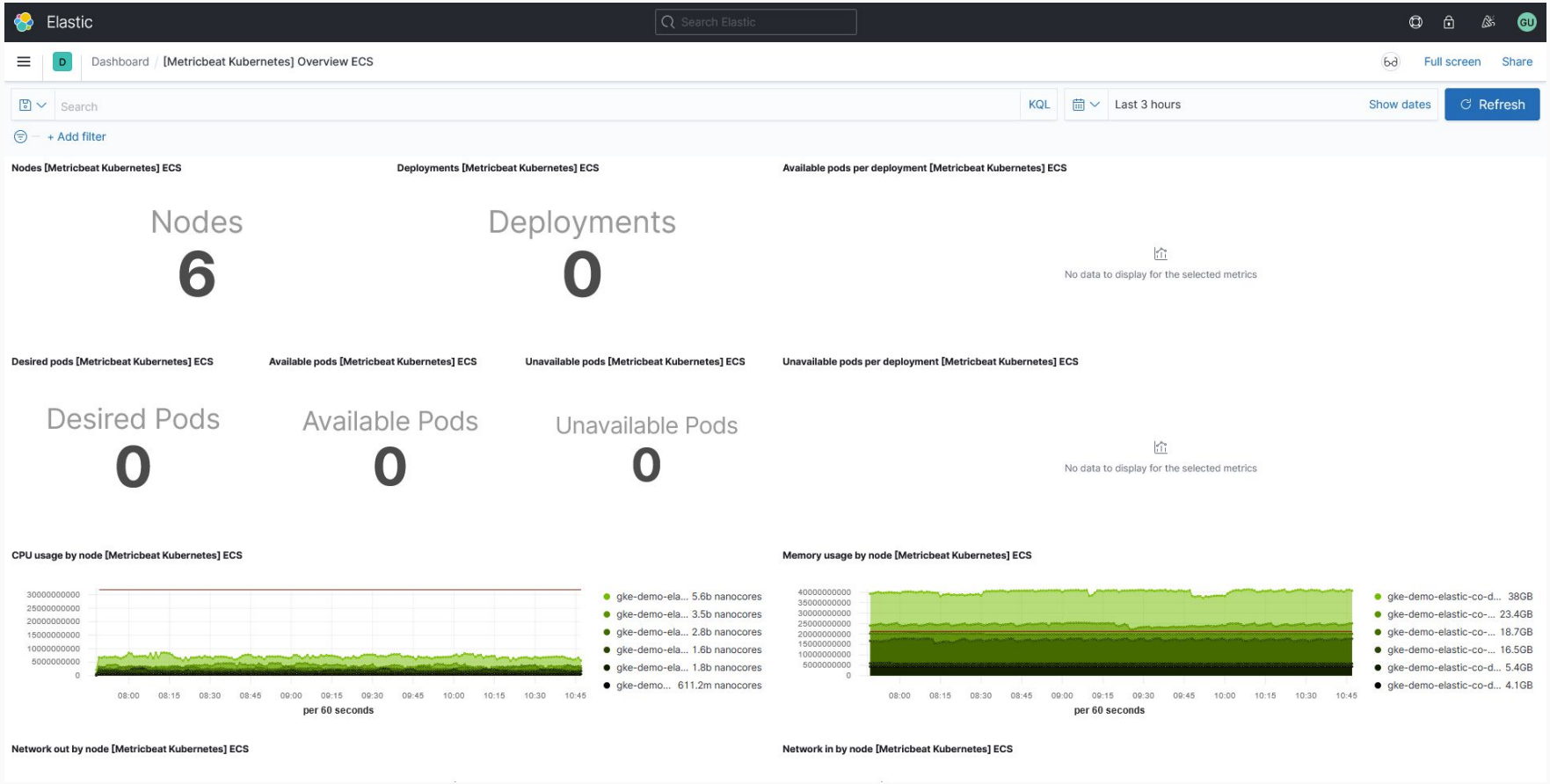
ELK Stack Getting Started

...sadly, we can’t do that on our VM due to limited resources

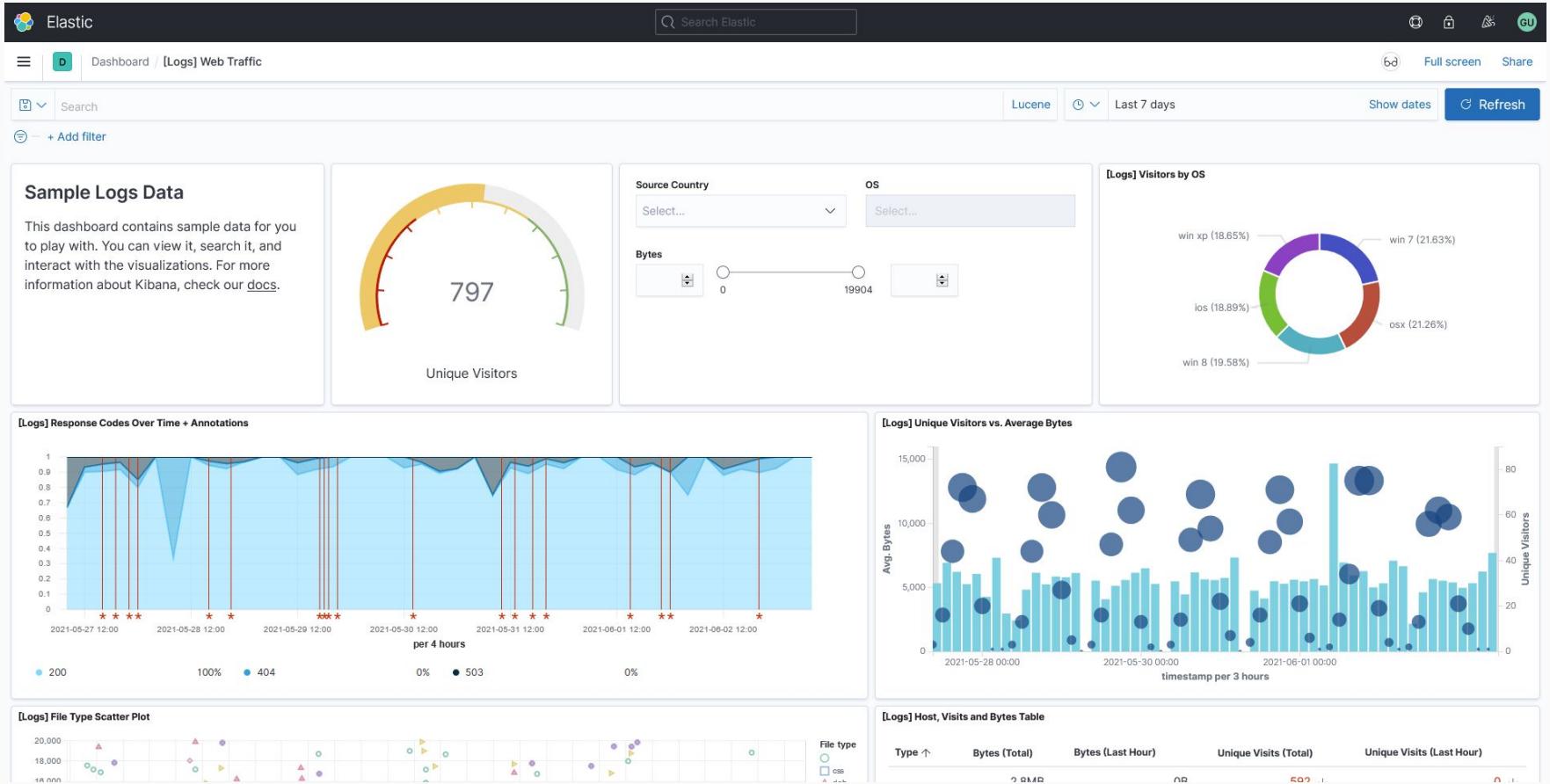
To run ELK stack, you should have multiple servers with 4 core / 4G RAM at least

Hands-on at Elastic Demo

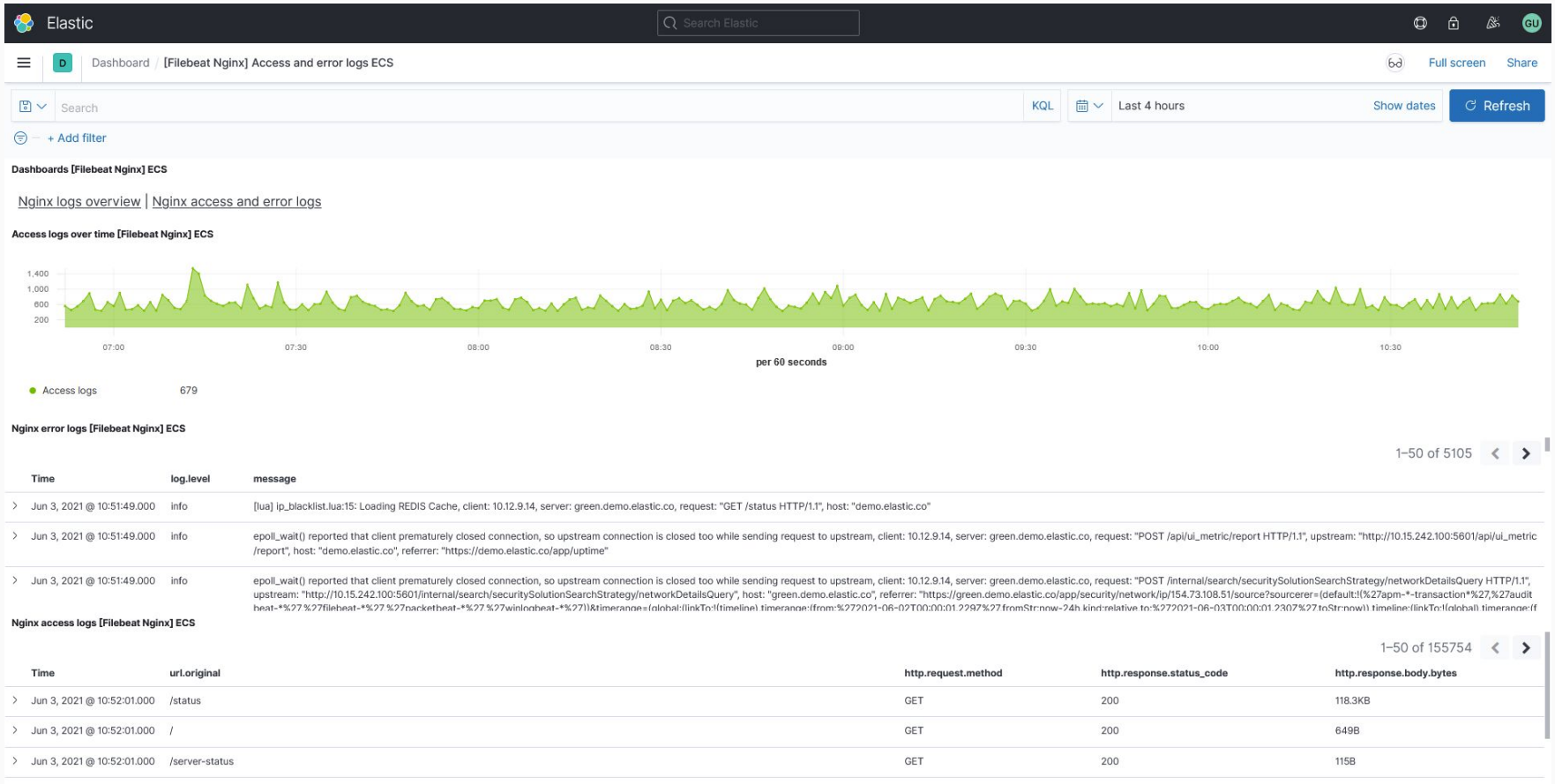
Kibana Demo - Metricbeat Kubernetes



Kibana Demo - Web Traffic



Kibana Demo - Nginx Log



Q & A