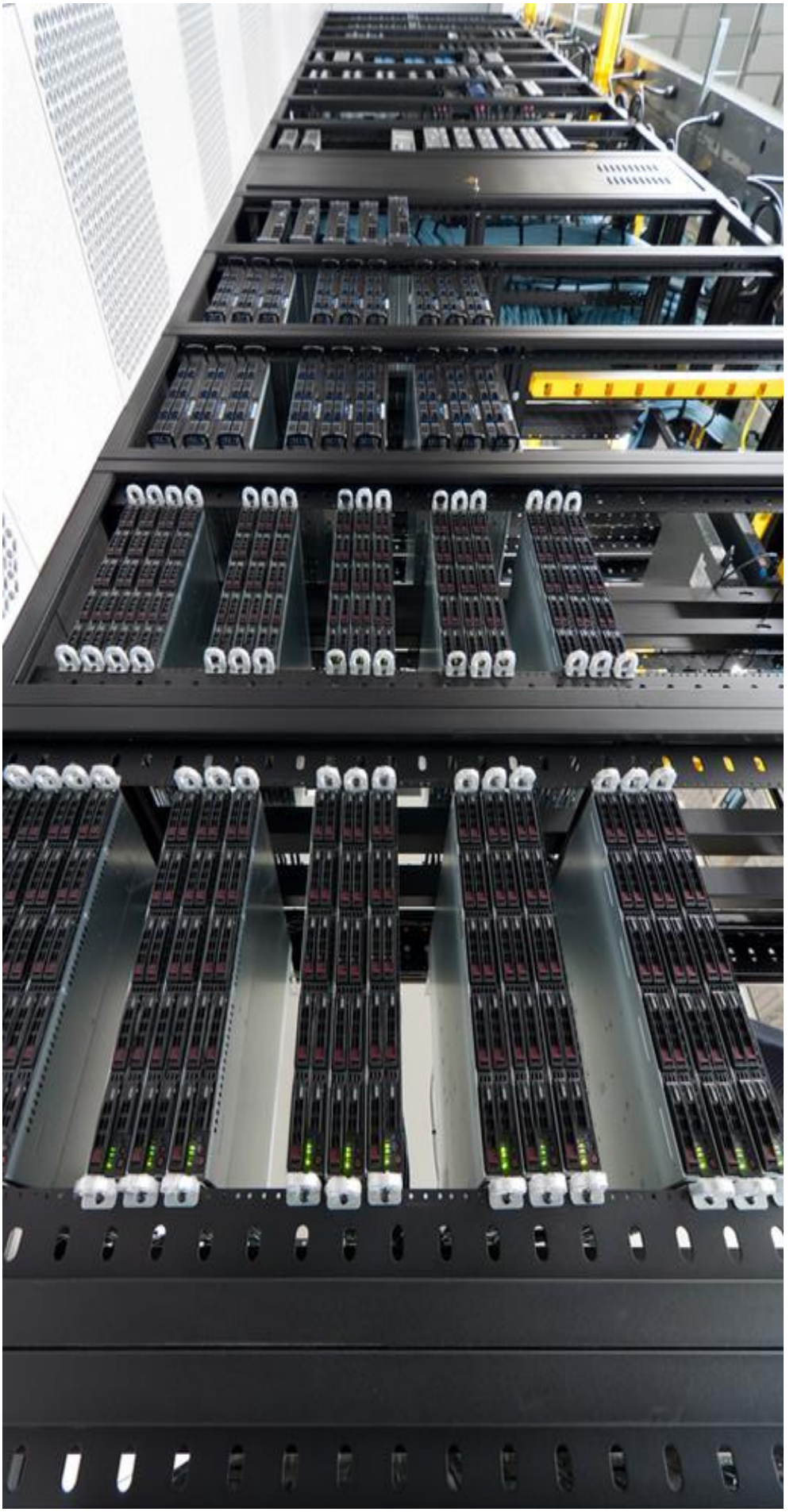
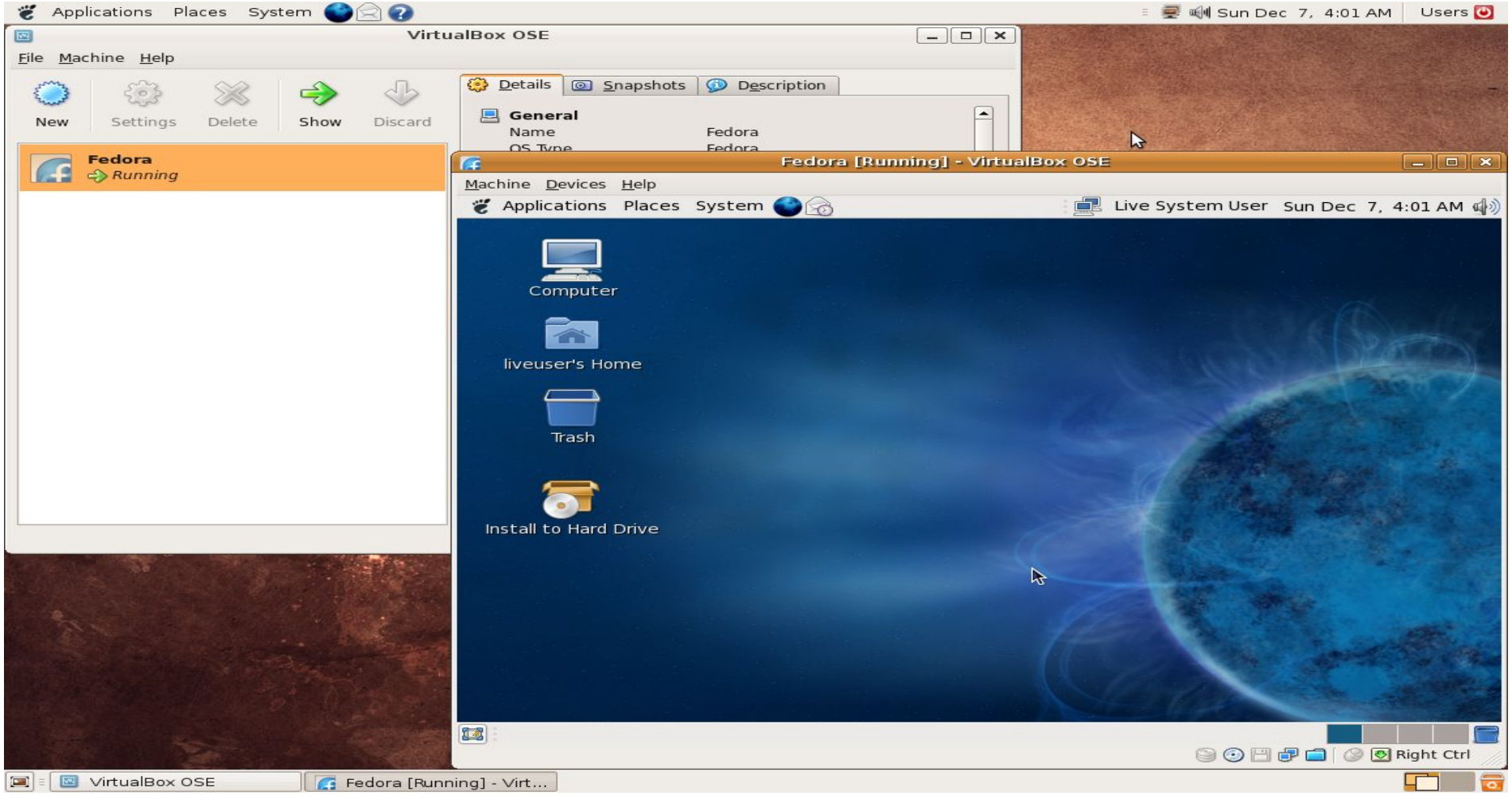
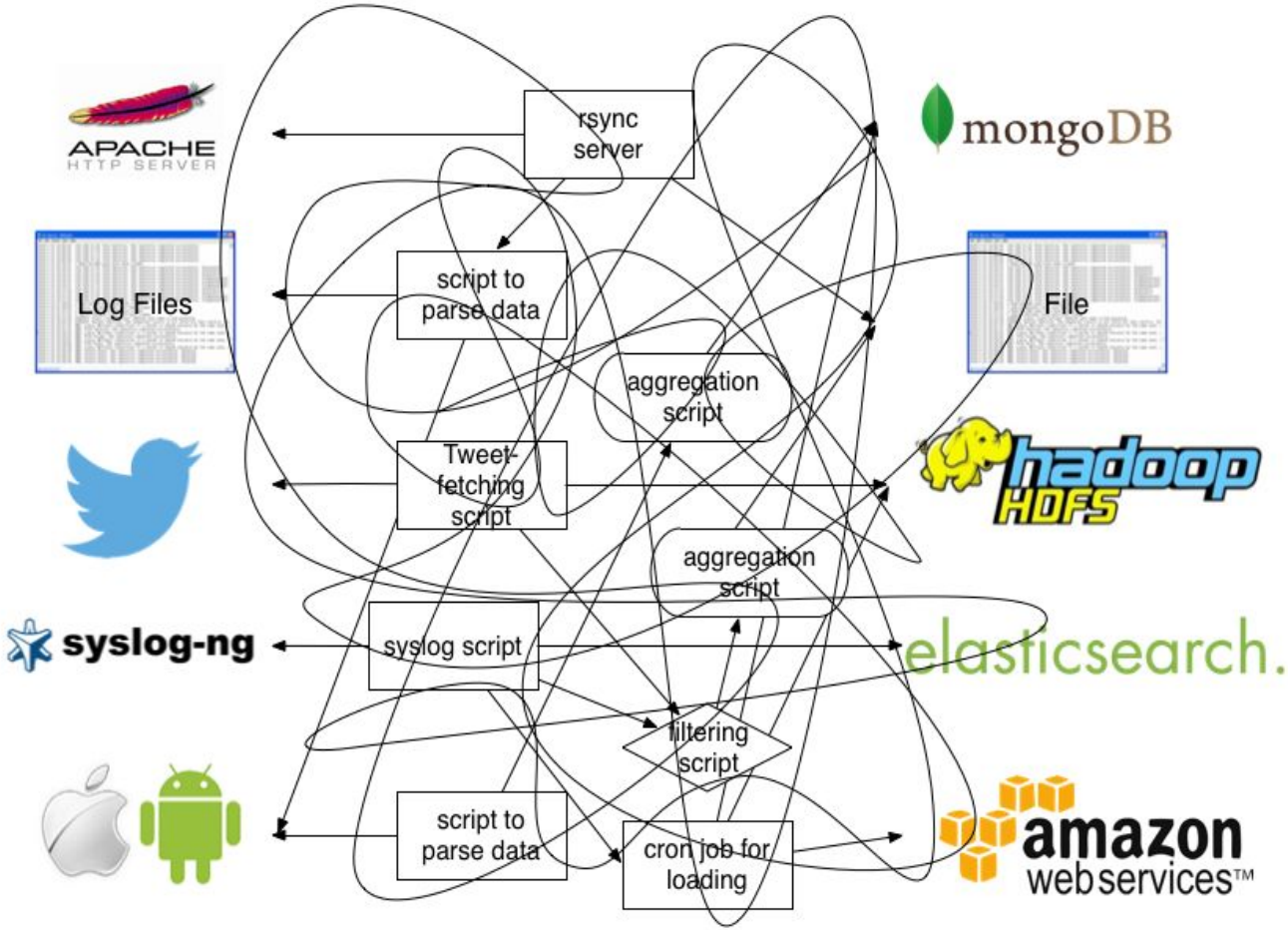
COMO MONTAR UMA INFRAESTRUTURA PARA ANÁLISE DE DADOS, 100% OPEN SOURCE EM MENOS DE 40 MINUTOS

eth0@papodesysadmin.org

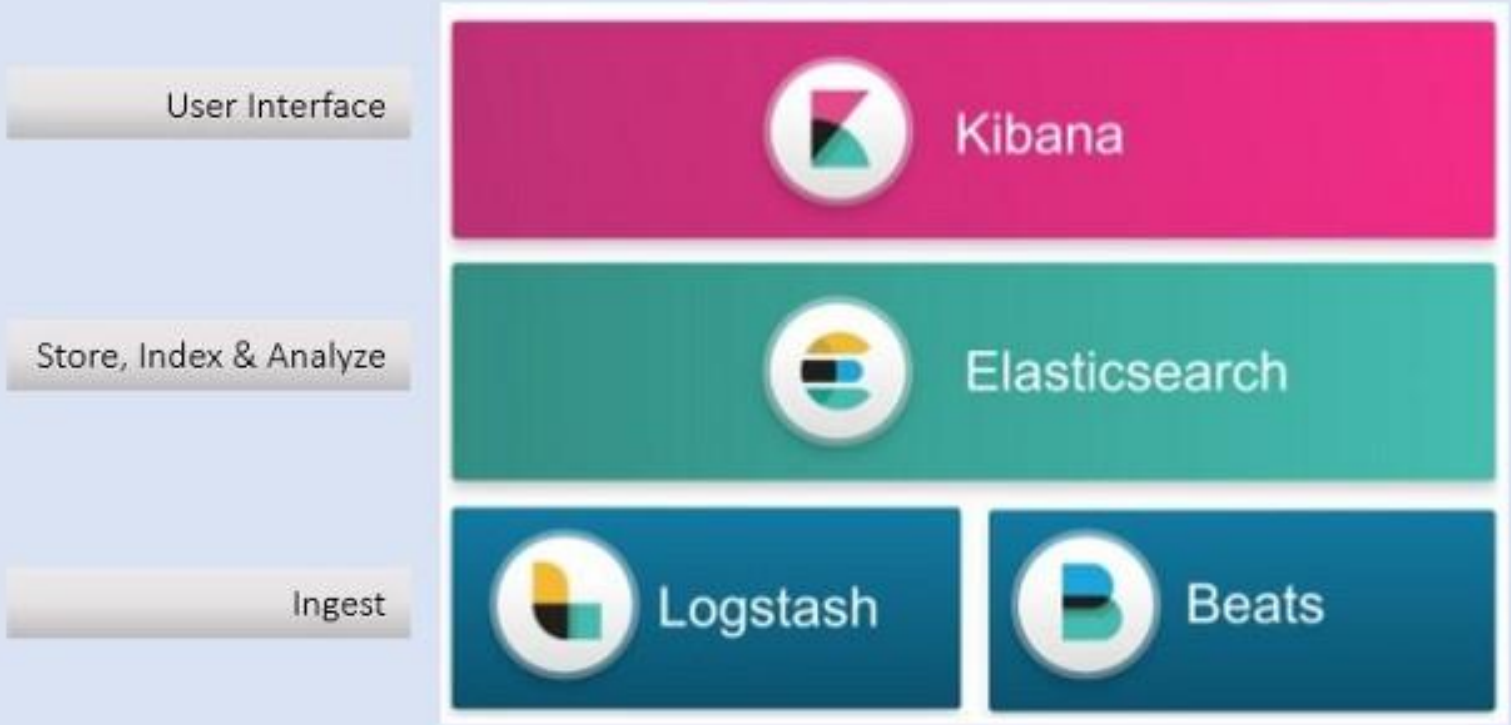



Applications
Places
System
Sun Dec 7, 4:01 AM
Users
VirtualBox OSE
File
Machine
Help
New
Settings
Delete
Show
Discard
Details
Snapshots
Description
General
Name
Fedora
Fedora
Running
Fedora [Running] - VirtualBox OSE
Machine
Devices
Help
Applications
Places
System
Live System User
Sun Dec 7, 4:01 AM
Computer
liveuser's Home
Trash
Install to Hard Drive
Right Ctrl
VirtualBox OSE
Fedora [Running] - Virt...

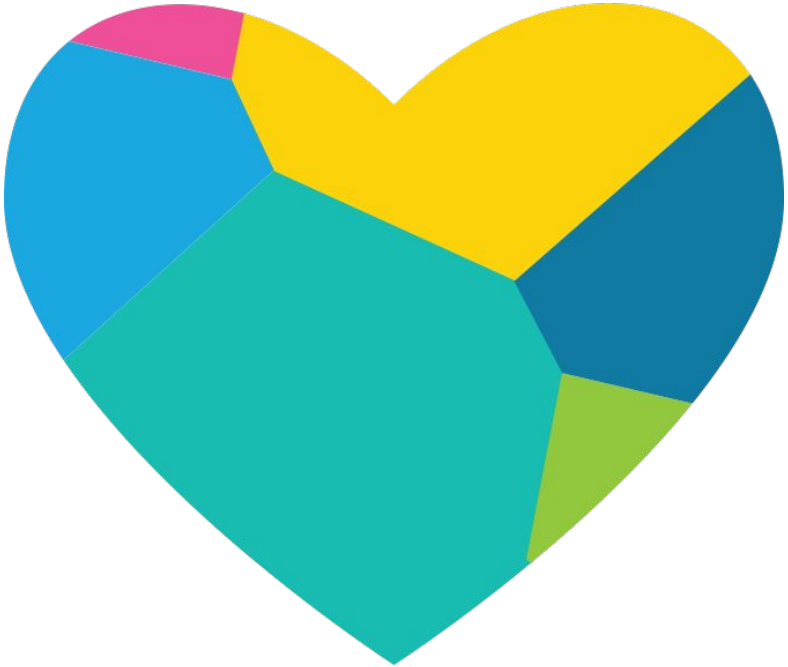

APACHE
HTTP SERVER
rsync server
mongoDB
Log Files
script to parse data
File
aggregation script
Tweet-fetching script
hadoop
HDFS
aggregation script
syslog-ng
syslog script
elasticsearch.
filtering script
script to parse data
cron job for loading
amazon
web services™

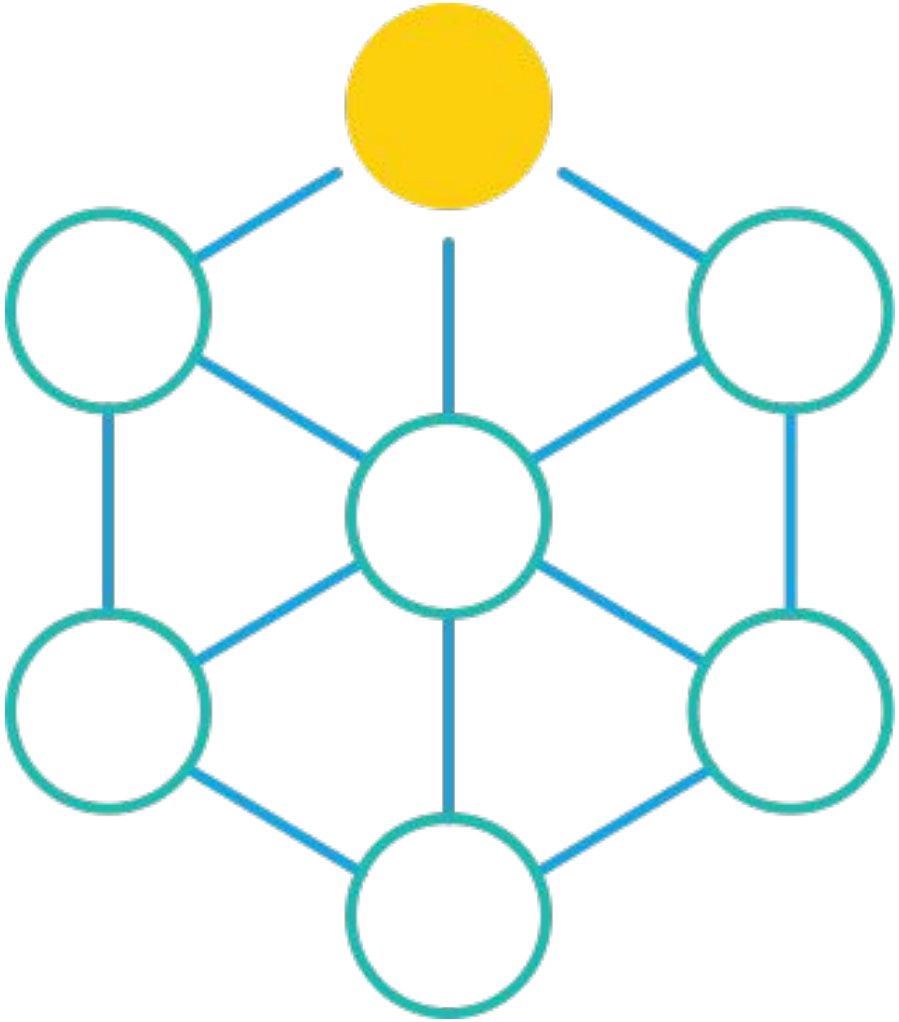

Data
Reporting
Analysis
Action
Value

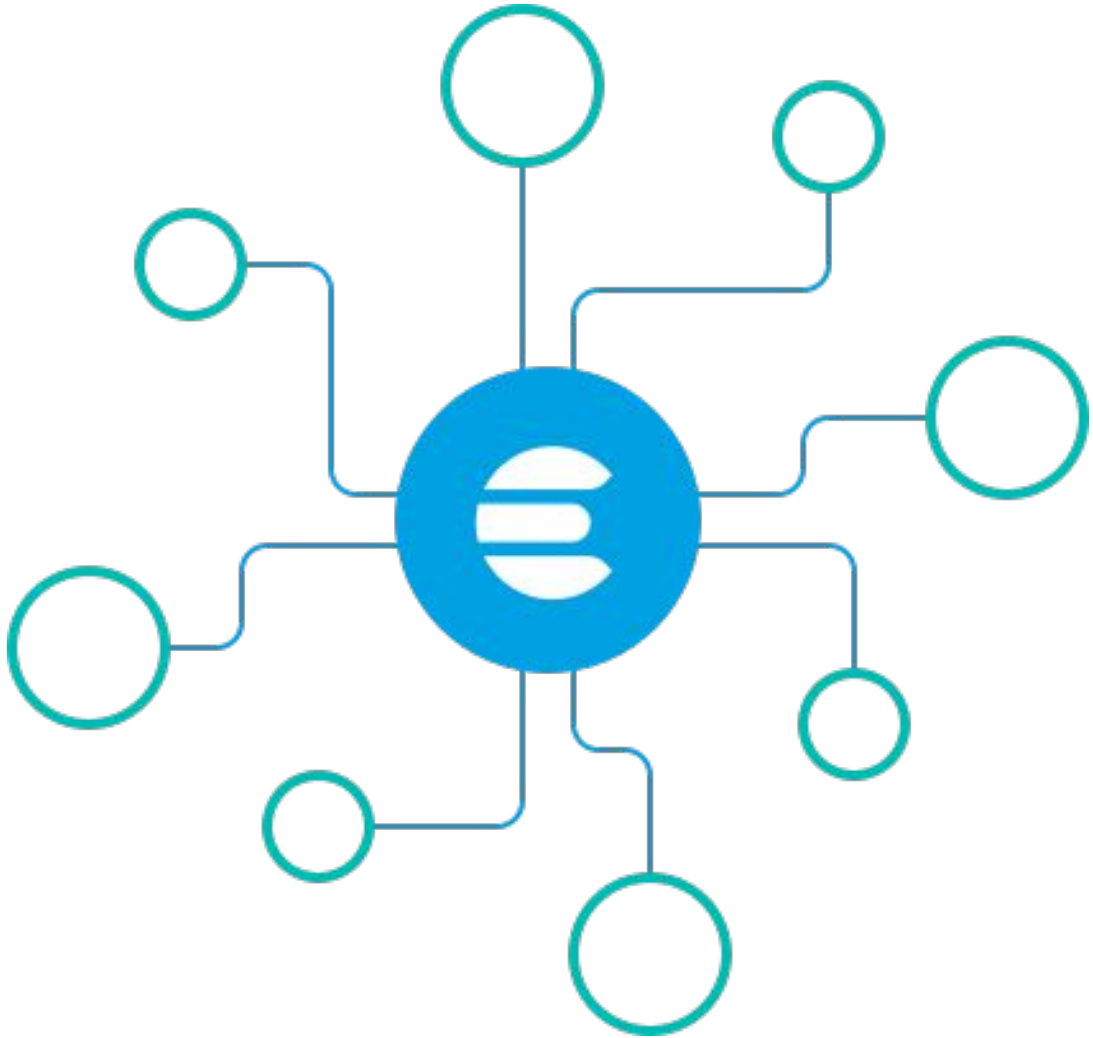
Elastic Stack



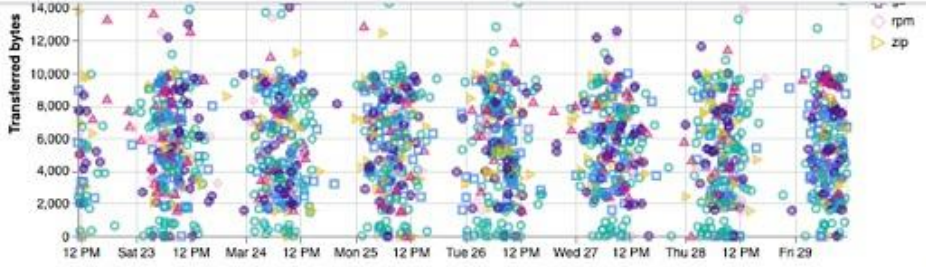
Elasticsearch





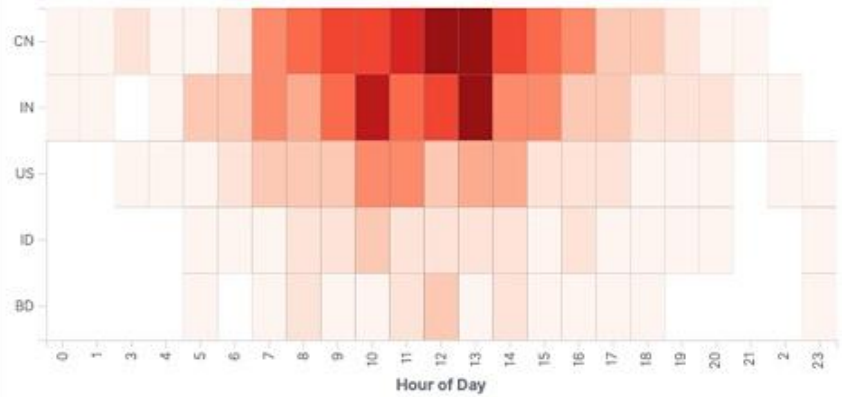


Kibana



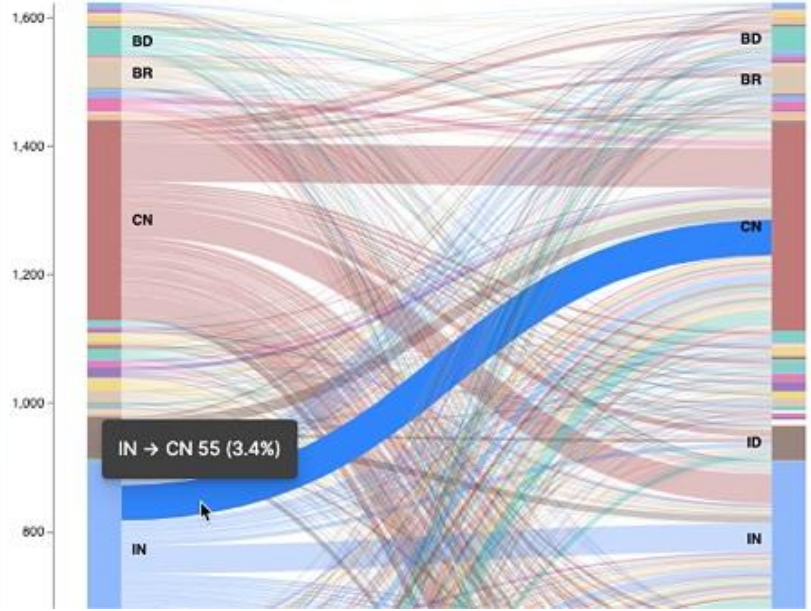
gz	1.594MB	34.493KB	283	7
css	1.385MB	12.378KB	270	2
zip	1.257MB	6.654KB	212	3
deb	1.085MB	6.844KB	173	1
rpm	458.989KB	0B	71	0

[Logs] Heatmap

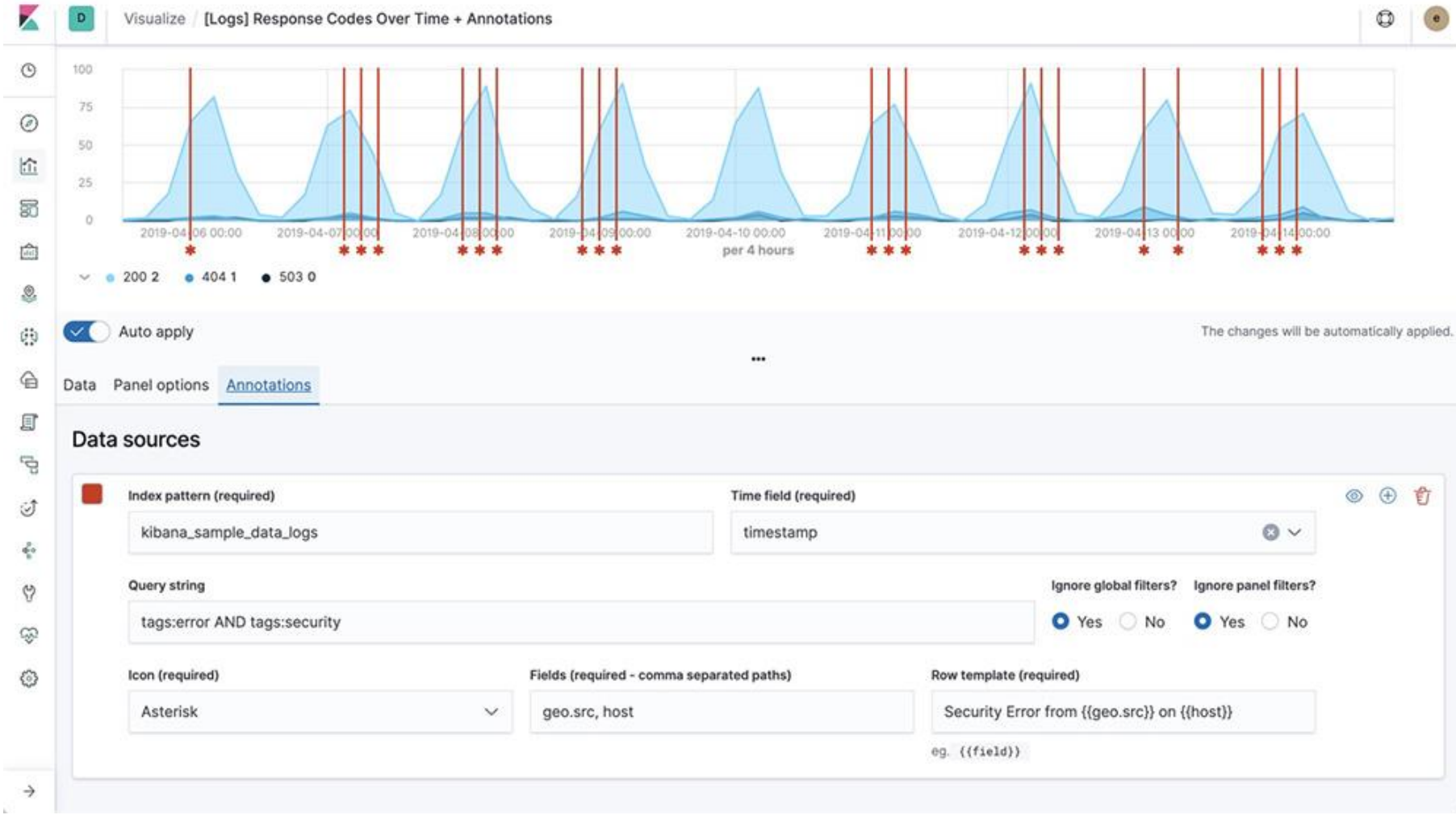


[Logs] Unique Visitors by Country

[Vega] Source and Destination Sankey Chart

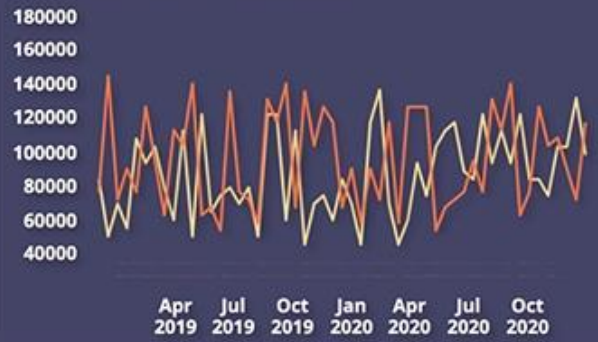



Visualize / [Logs] Unique Visitors by Country
Save Share Inspect Refresh
Filters Search KQL Last 7 days Show dates Refresh
+ Add filter
Unique Visitors
5 – 69
69 – 133
133 – 197
197 – 261
© OpenStreetMap contributors, Elastic Maps Service , Made with NaturalEarth


Visualize / [Logs] Response Codes Over Time + Annotations
100
75
50
25
0
2019-04-06 00:00
2019-04-07 00:00
2019-04-08 00:00
2019-04-09 00:00
2019-04-10 00:00
2019-04-11 00:00
2019-04-12 00:00
2019-04-13 00:00
2019-04-14 00:00
per 4 hours
200 2
404 1
503 0
Auto apply
The changes will be automatically applied.
Data
Panel options
Annotations
Data sources
Index pattern (required)
kibana_sample_data_logs
Time field (required)
timestamp
Query string
tags:error AND tags:security
Ignore global filters?
Yes
No
Ignore panel filters?
Yes
No
Icon (required)
Asterisk
Fields (required - comma separated paths)
geo.src, host
Row template (required)
Security Error from {{geo.src}} on {{host}}
eg. {{field}}

Order Tracking

New Orders vs. Filled Orders



Orders by Status

Total Cost of Shipping

$79475.00

Return Shipping Cost

$5324.83

Average Bill Rate Per Mile

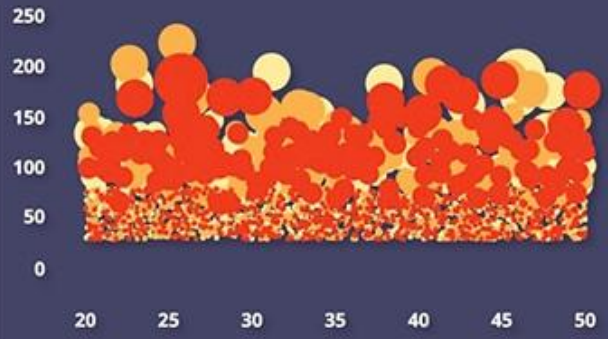
$0.05

Return Rate

6.7%

0.2%

Time to Fill Orders



Paid Subscribers

3132.3

Minutes

Average Time to Fill Order

23.4

Minutes

On Time Delivery

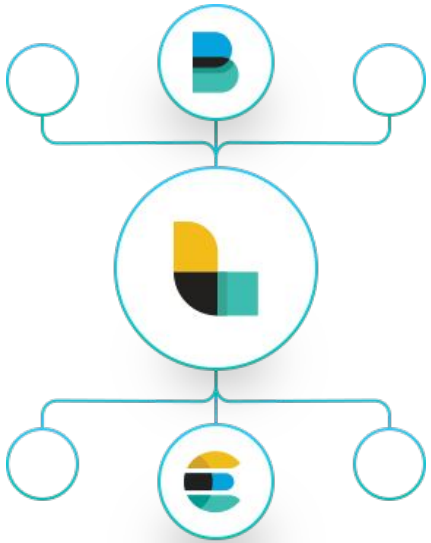
Lost Orders

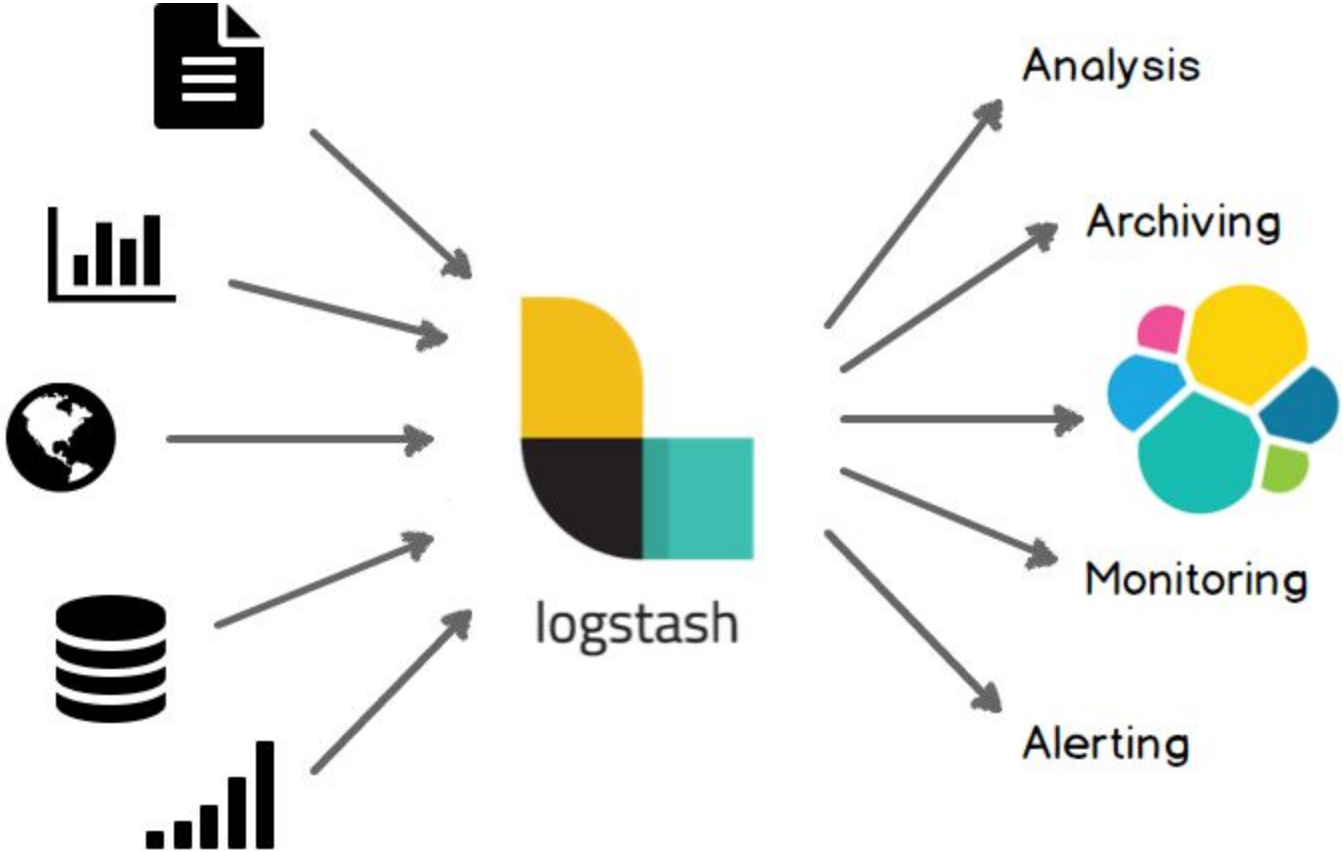
4

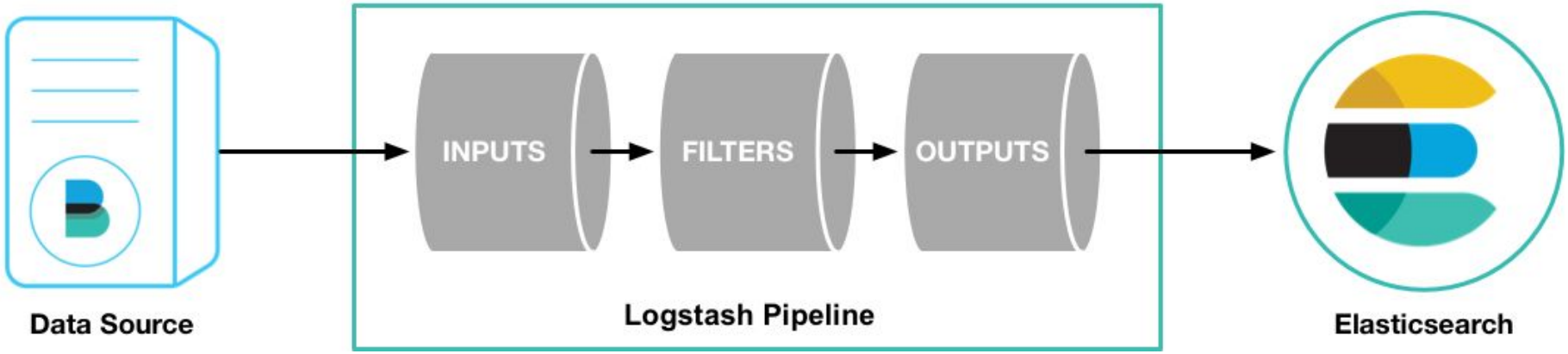
Total Shipment Count

107525

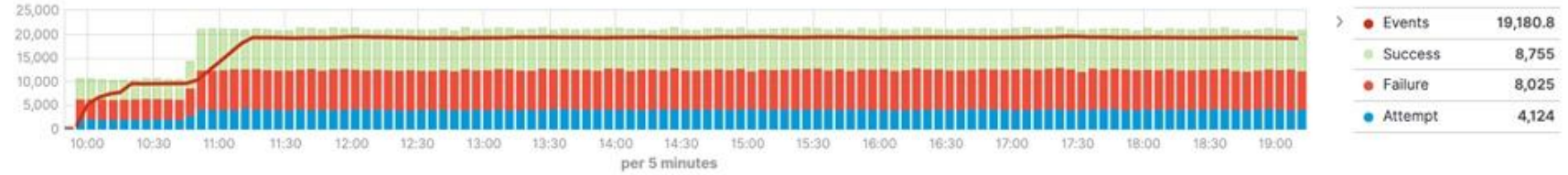
Logstash



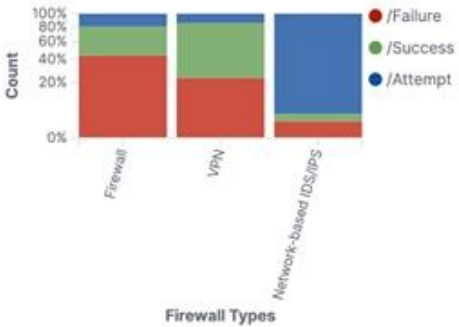

Analysis
Archiving
Monitoring
Alerting
logstash


INPUTS
FILTERS
OUTPUTS
Data Source
Logstash Pipeline
Elasticsearch

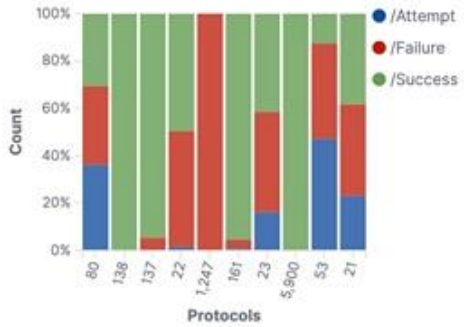
Events by Outcome [ArcSight]



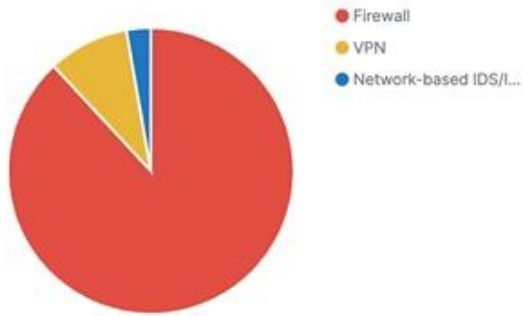
Outcome by Device Type [ArcSight]



Destination Ports by Outcome [ArcSight]



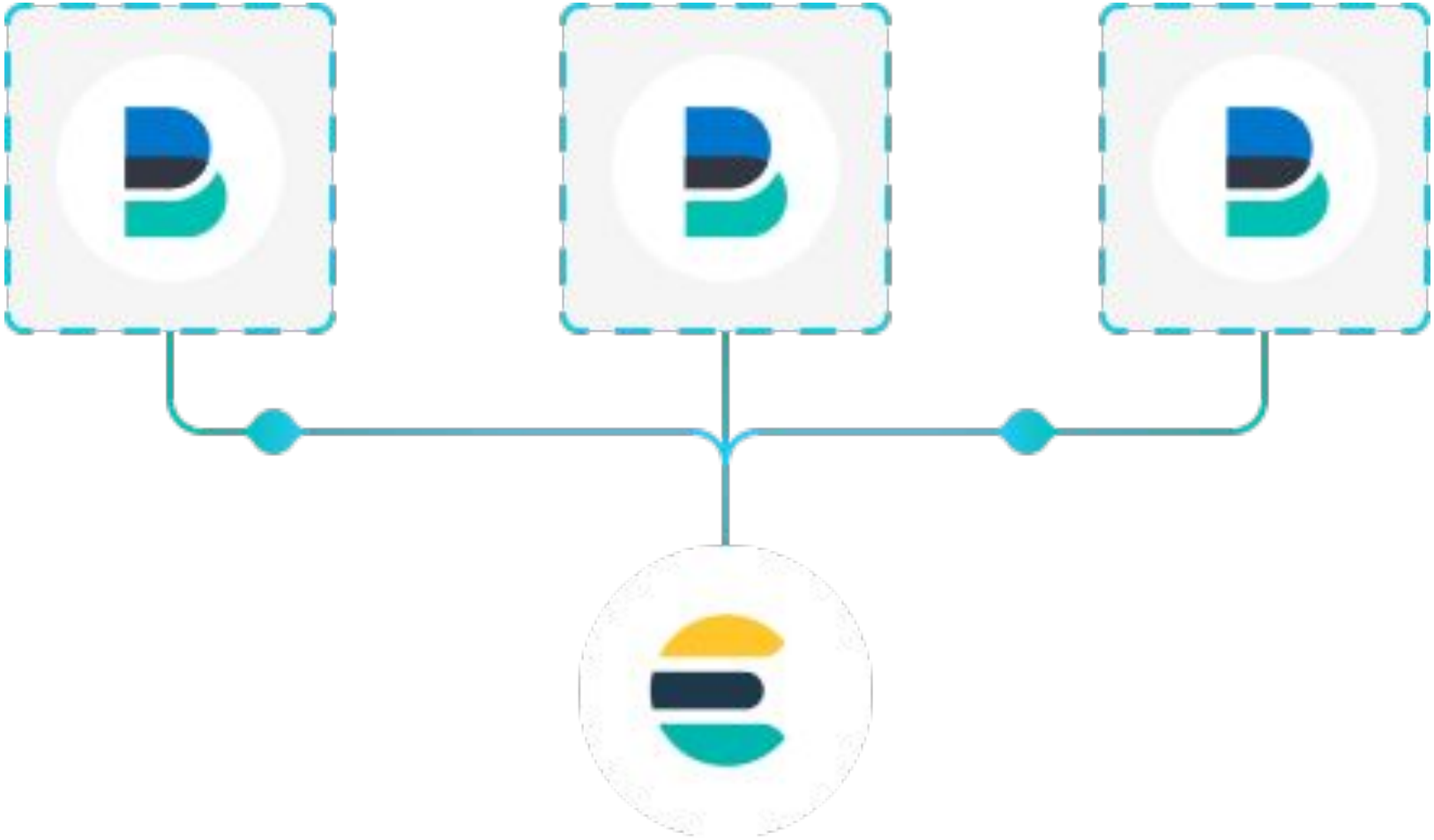
Device Type Breakdown [ArcSight]

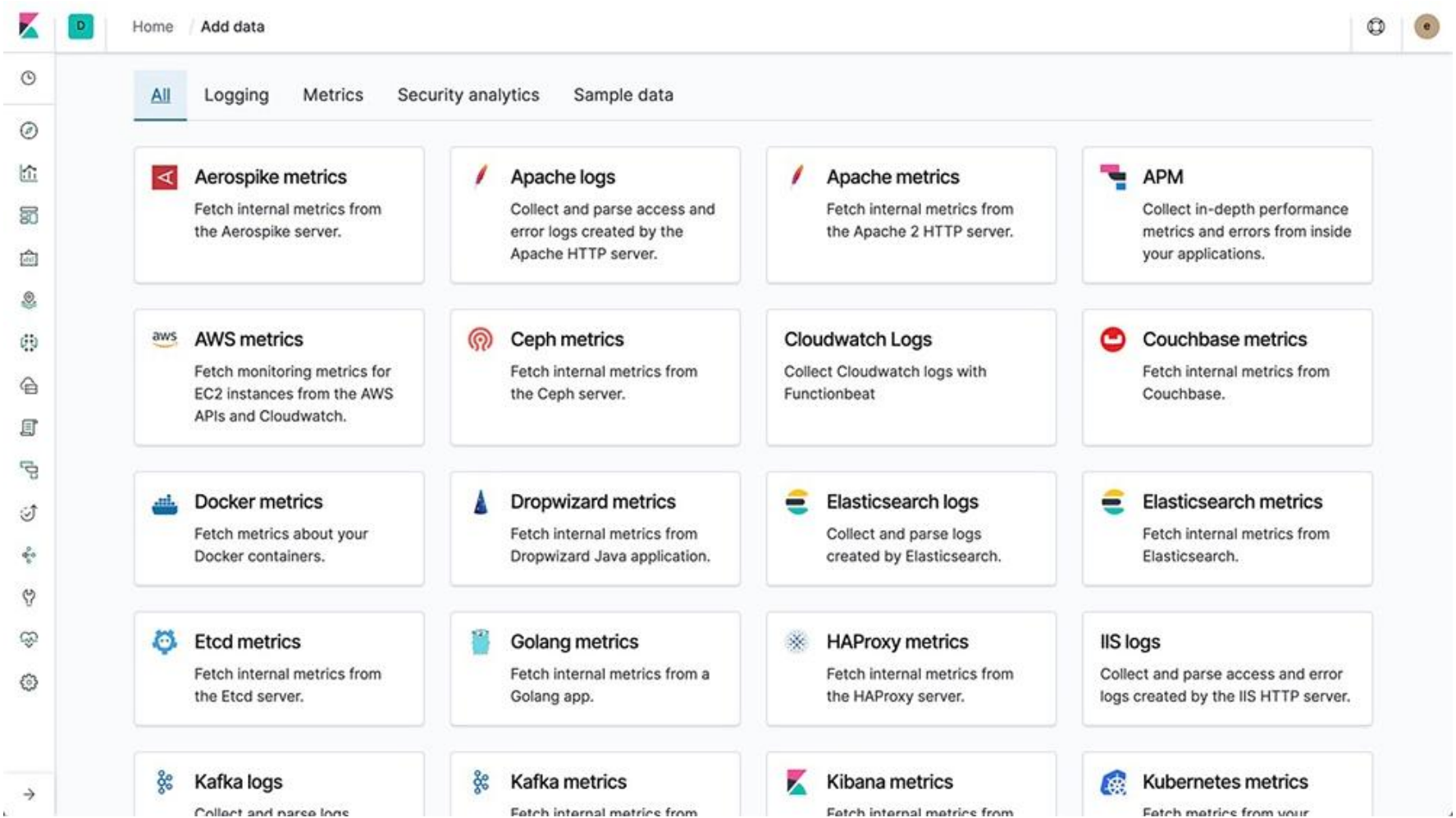


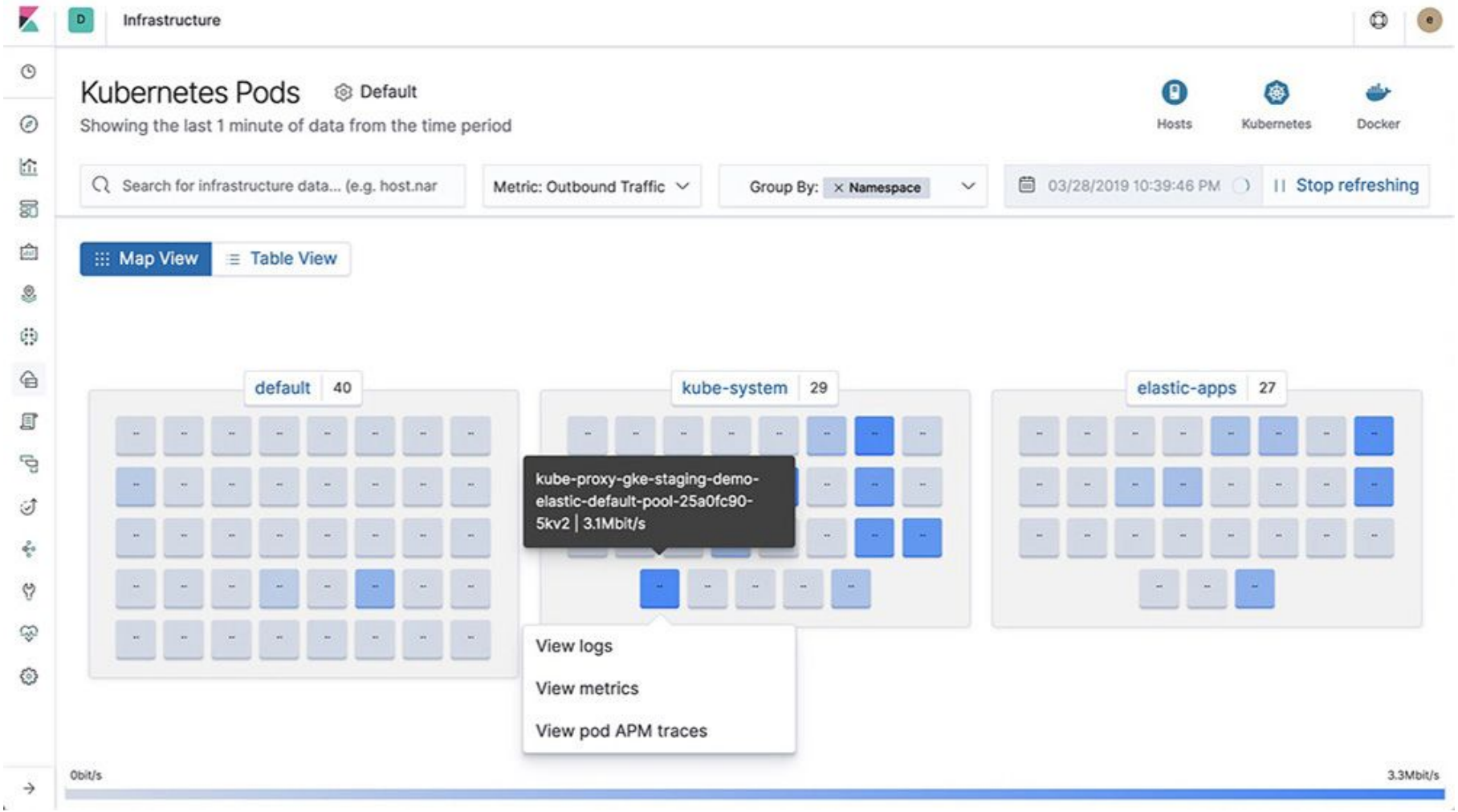
Top 10 Application Protocols [ArcSight]

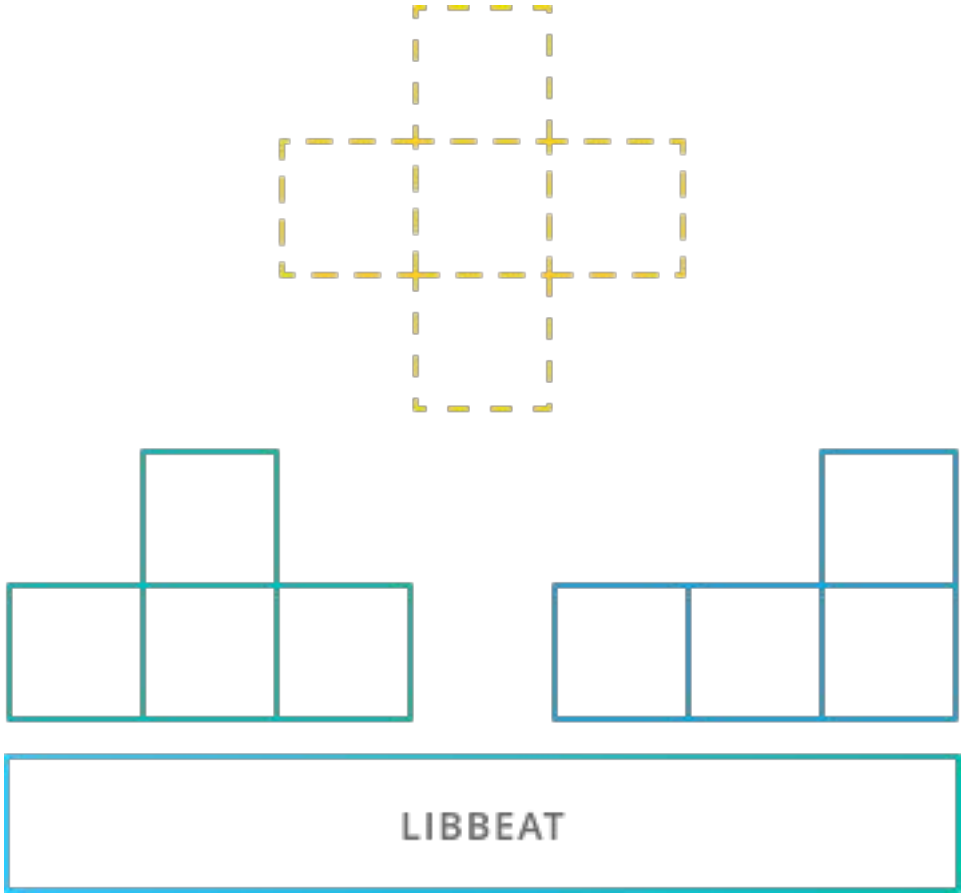
applicationProtocol: Descending - Count

Beats




Home / Add data
All
Logging
Metrics
Security analytics
Sample data
Aerospike metrics
Fetch internal metrics from the Aerospike server.
Apache logs
Collect and parse access and error logs created by the Apache HTTP server.
Apache metrics
Fetch internal metrics from the Apache 2 HTTP server.
APM
Collect in-depth performance metrics and errors from inside your applications.
AWS metrics
Fetch monitoring metrics for EC2 instances from the AWS APIs and Cloudwatch.
Ceph metrics
Fetch internal metrics from the Ceph server.
Cloudwatch Logs
Collect Cloudwatch logs with Functionbeat
Couchbase metrics
Fetch internal metrics from Couchbase.
Docker metrics
Fetch metrics about your Docker containers.
Dropwizard metrics
Fetch internal metrics from Dropwizard Java application.
Elasticsearch logs
Collect and parse logs created by Elasticsearch.
Elasticsearch metrics
Fetch internal metrics from Elasticsearch.
Etcd metrics
Fetch internal metrics from the Etcd server.
Golang metrics
Fetch internal metrics from a Golang app.
HAProxy metrics
Fetch internal metrics from the HAProxy server.
IIS logs
Collect and parse access and error logs created by the IIS HTTP server.
Kafka logs
Kafka metrics
Kibana metrics
Kubernetes metrics


Infrastructure
Kubernetes Pods
Default
Showing the last 1 minute of data from the time period
Hosts
Kubernetes
Docker
Search for infrastructure data... (e.g. host.nar
Metric: Outbound Traffic
Group By:
Namespace
03/28/2019 10:39:46 PM
Stop refreshing
Map View
Table View
default 40
kube-system 29
elastic-apps 27
kube-proxy-gke-staging-demo-elastic-default-pool-25a0fc90-5kv2 | 3.1Mbit/s
View logs
View metrics
View pod APM traces
0bit/s
3.3Mbit/s


LIBBEAT

Eduardo Neves

Elastic Stack Specialist | Mentor

DevOps | SRE | Application Security

papo de

sysadmin