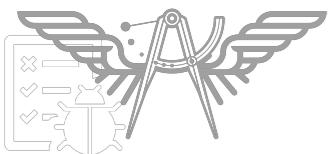


สยามชามนกิจ
SIAM CHAMNANKIT KIT

Kibana





Somkiat Puisungnoen

Somkiat Puisungnoen

Update Info 1 View Activity Log 10+ ...

Timeline About Friends 3,138 Photos More

When did you work at Opendream? X

... 22 Pending Items

Intro

Software Craftsmanship

Software Practitioner at สยามชัมนาณกิจ พ.ศ. 2556

Agile Practitioner and Technical at SPRINT3r

Post Photo/Video Live Video Life Event

What's on your mind?

Public Post

Somkiat Puisungnoen 15 mins · Bangkok · ⚙️

Java and Bigdata





Page

Messages

Notifications 3

Insights

Publishing Tools

Settings

Help ▾



somkiat.cc

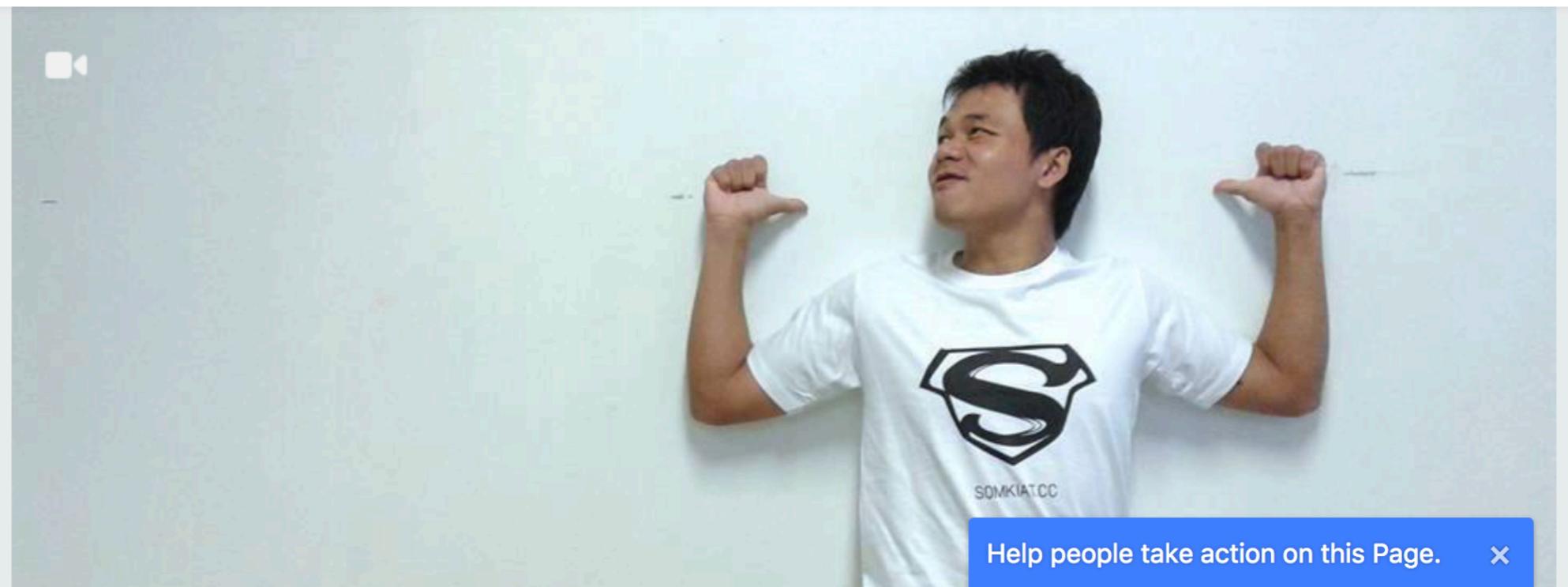
@somkiat.cc

Home

Posts

Videos

Photos



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

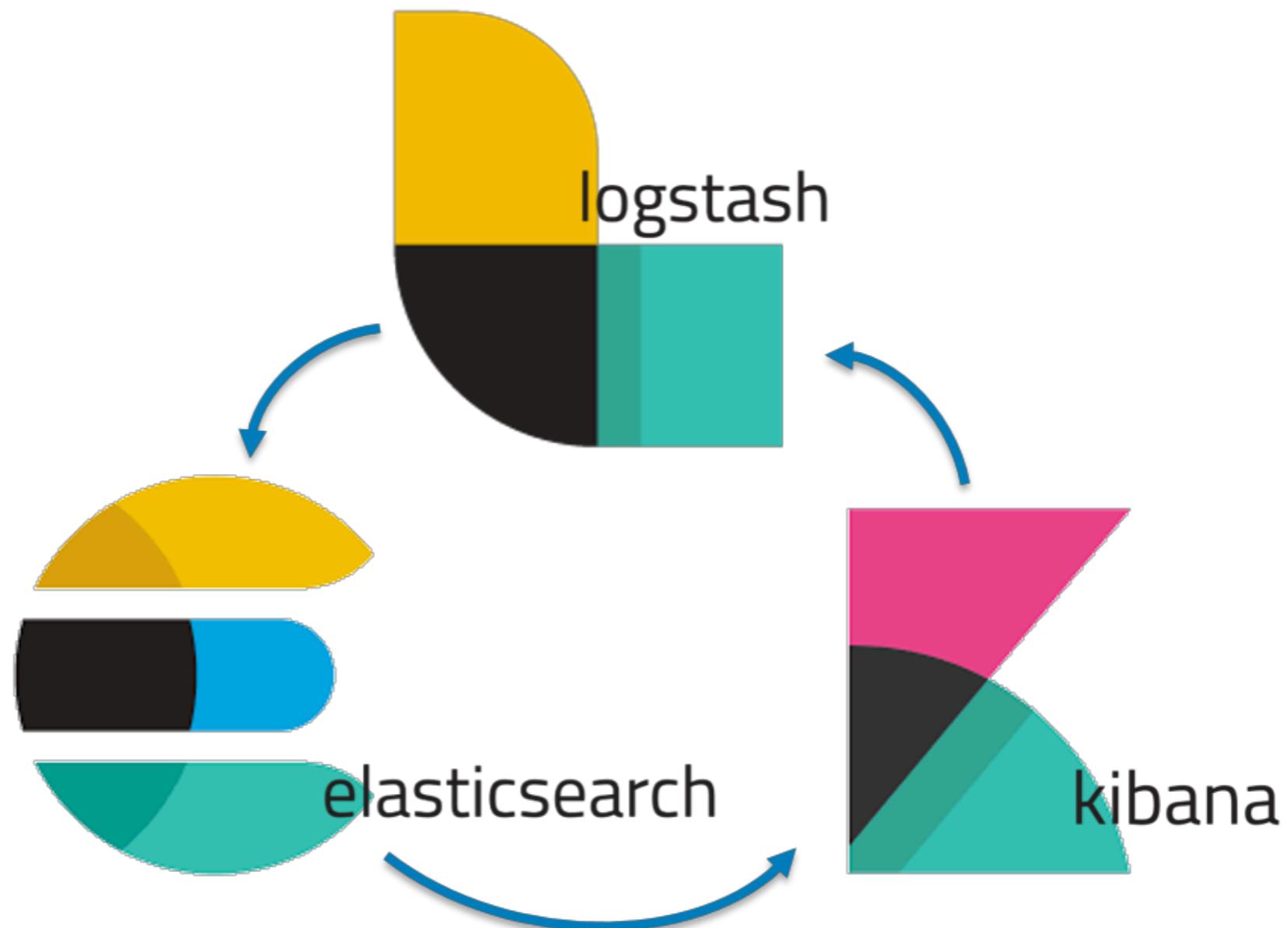
https://github.com/up1/course_elk



Agenda

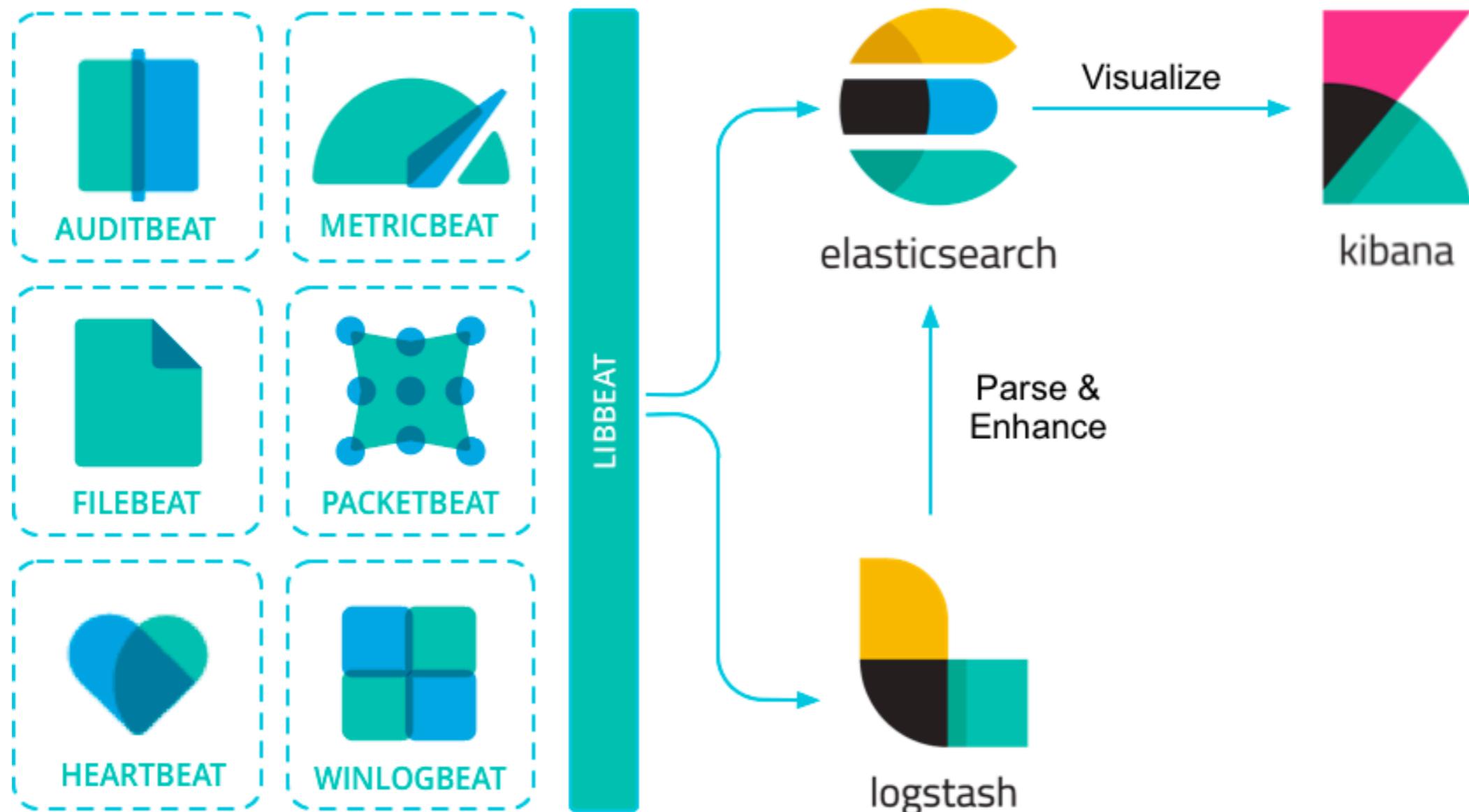
- Working with Kibana
- Working with Logstash/Beat
- Monitoring with Kibana







Beat



<https://www.elastic.co/guide/en/beats/libbeat/current/index.html>



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Beat

Purpose	Library
Audit data	Auditbeat
Log files	Filebeat
Cloud data	Functionbeat
Availability	Heartbeat
Metrics	Metricbeat
Network traffic	Packetbeat
Windows event logs	Winlogbeat

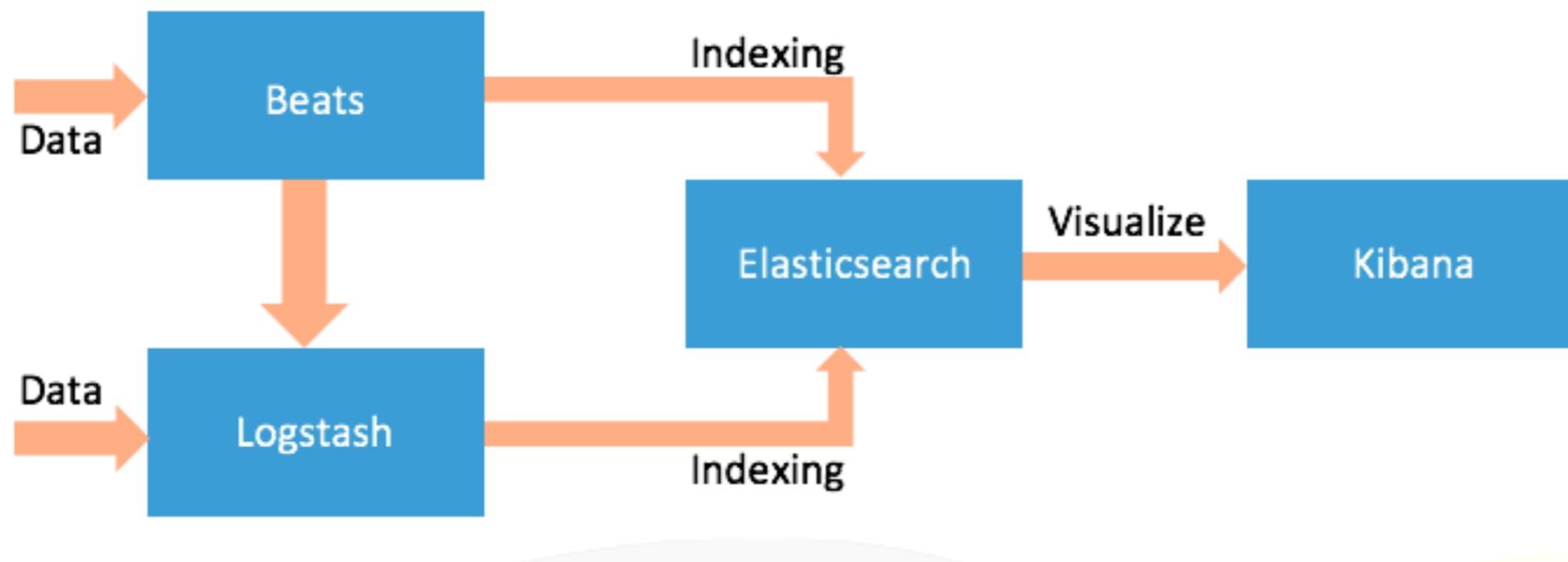
<https://www.elastic.co/guide/en/beats/libbeat/current/beats-reference.html>



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

ELK stack



Kibana



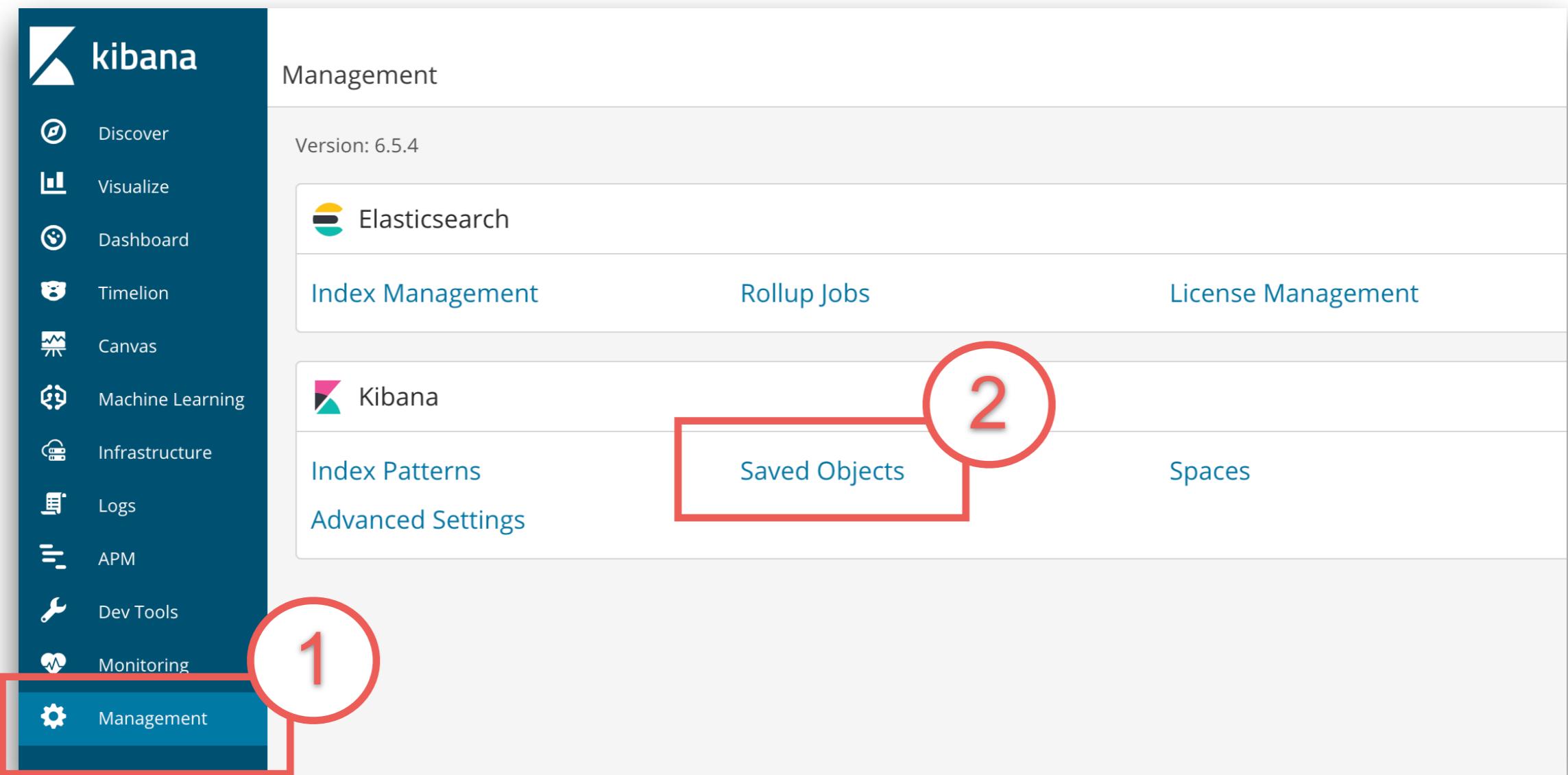
Kibana

Create visualization
Create dashboard
Infrastructure
Monitoring



Import/Export

Go to management menu => Saved Objects



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Import/Export

Working with JSON file

Saved Objects

From here you can delete saved objects, such as saved searches. You can also edit the raw data of saved objects. Typically objects are only modified via their associated application, which is probably what you should use instead of this screen.

<input type="checkbox"/>	Type	Title	<input type="button" value="Type"/>	<input type="button" value="Delete"/>	<input type="button" value="Export"/>
<input type="checkbox"/>	File	D1			
<input checked="" type="checkbox"/>	File	[Logs] Web Traffic			
<input type="checkbox"/>	File	store			
<input type="checkbox"/>	File	kibana_sample_data_logs			
<input type="checkbox"/>	File	S1			
<input type="checkbox"/>	File	G1			
<input type="checkbox"/>	File	[Logs] Unique Visitors vs. Average Bytes			
<input type="checkbox"/>	File	[Logs] Unique Visitors by Country			



BETA

Infrastructure with Kibana

Elasticsearch and Kibana 6.5 +



Setup instruction

The screenshot shows the Kibana interface. On the left is a sidebar with various navigation options: Discover, Visualize, Dashboard, Timelion, Canvas, Machine Learning, Infrastructure, Logs, APM, Dev Tools, Monitoring, and Management. The 'Logs' option is highlighted with a red box and a red circle containing the number '1'. The main content area displays a message: "Looks like you don't have any metrics indices." Below this message is a button labeled "Setup Instructions". This button is also highlighted with a red box and a red circle containing the number '2'.

Looks like you don't have any metrics indices.

Let's add some!

Setup Instructions



Add data to Kibana

Kibana Home Add Data to Kibana

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.
- Ceph metrics Fetch internal metrics from the Ceph server.
- 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.
- Etcdb metrics Fetch internal metrics from the Etcdb 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 Collect and parse logs created by Kafka.
- Kafka metrics Fetch internal metrics from the Kafka server.



Monitor your infrastructure

Monitor hosts and containers

View metrics

View logs

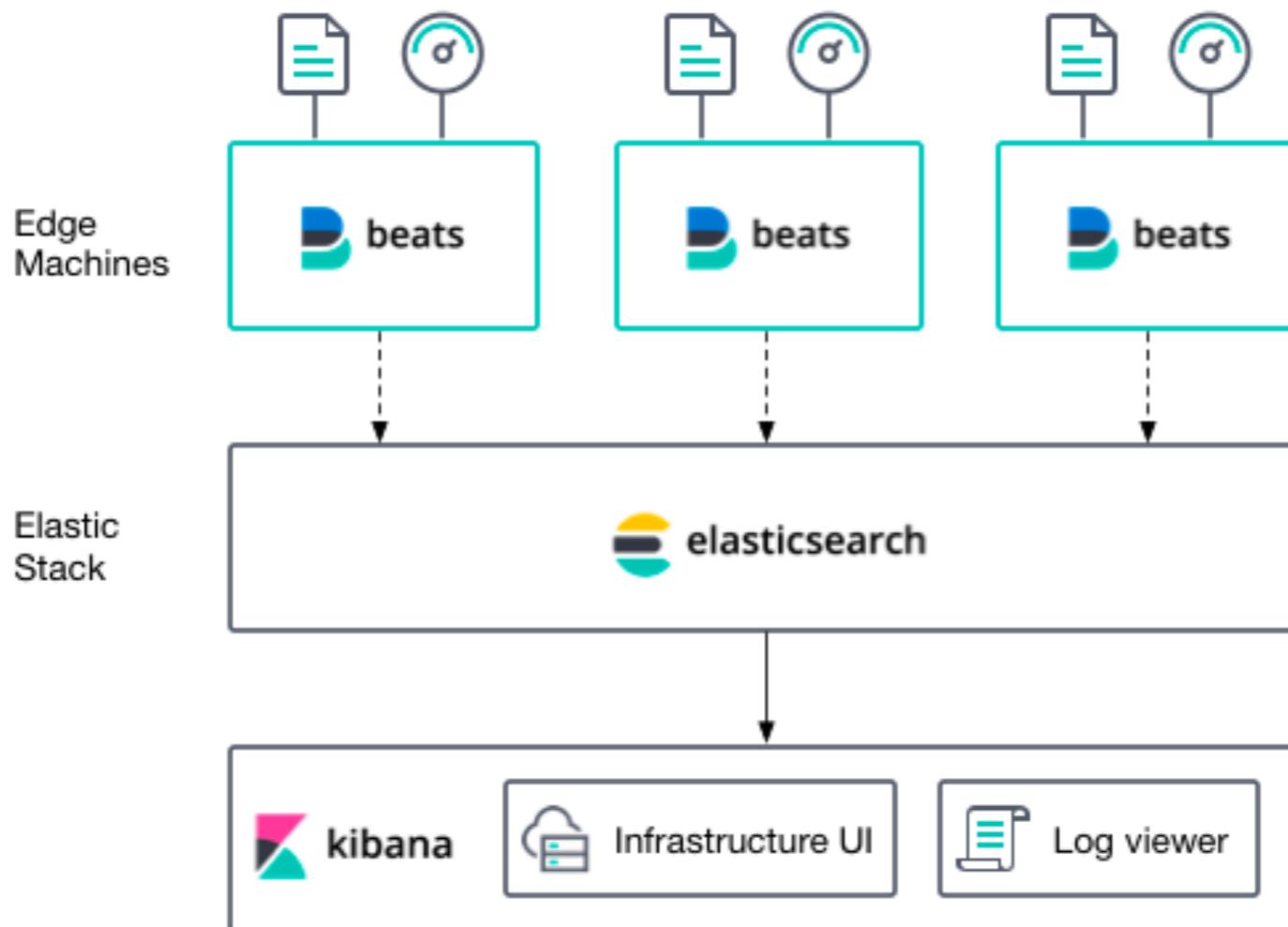
<https://www.elastic.co/guide/en/kibana/current/monitor-infra.html>



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Infrastructure monitoring



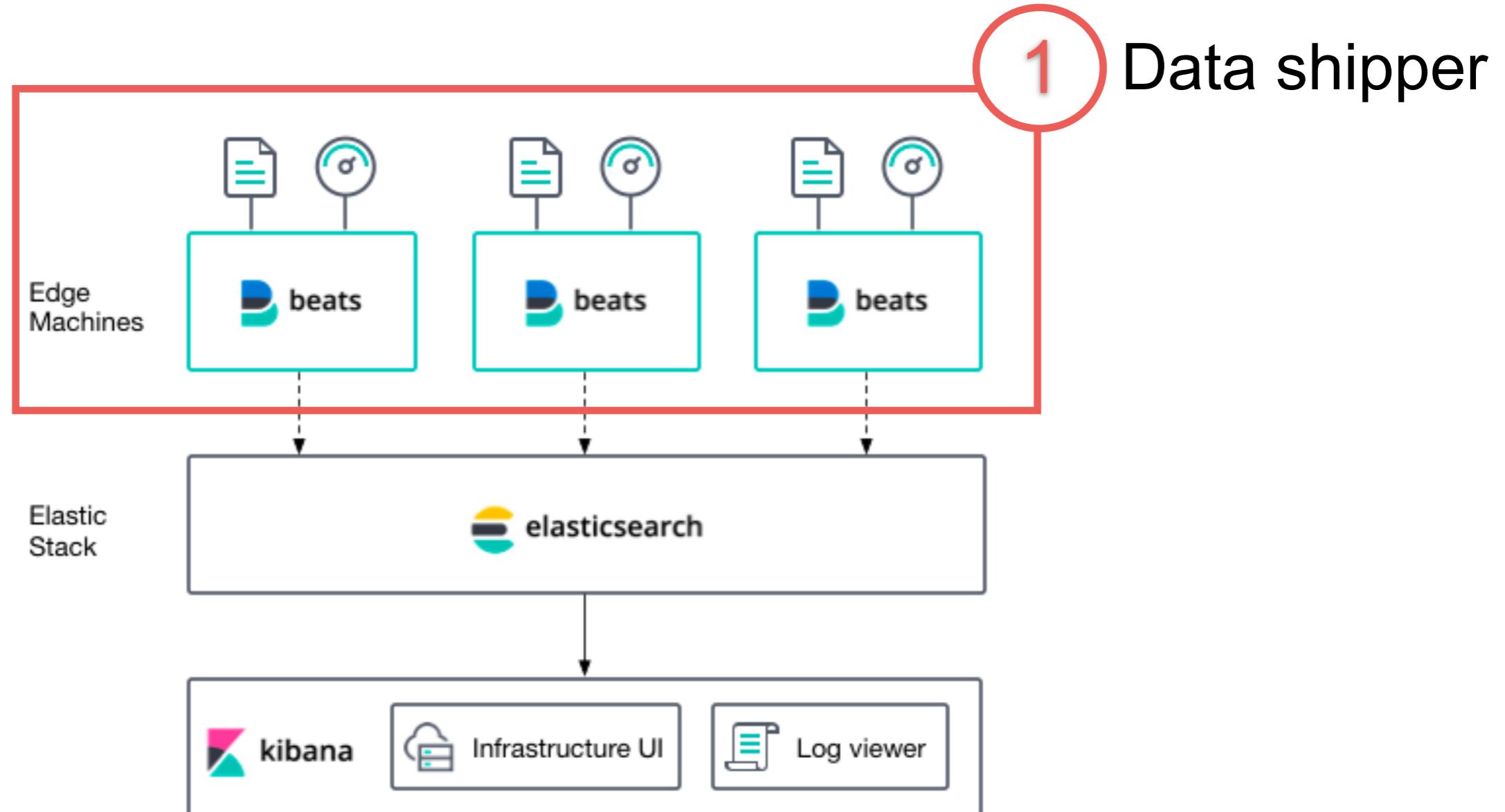
<https://www.elastic.co/guide/en/infrastructure/guide/6.5/infrastructure-monitoring-overview.html>



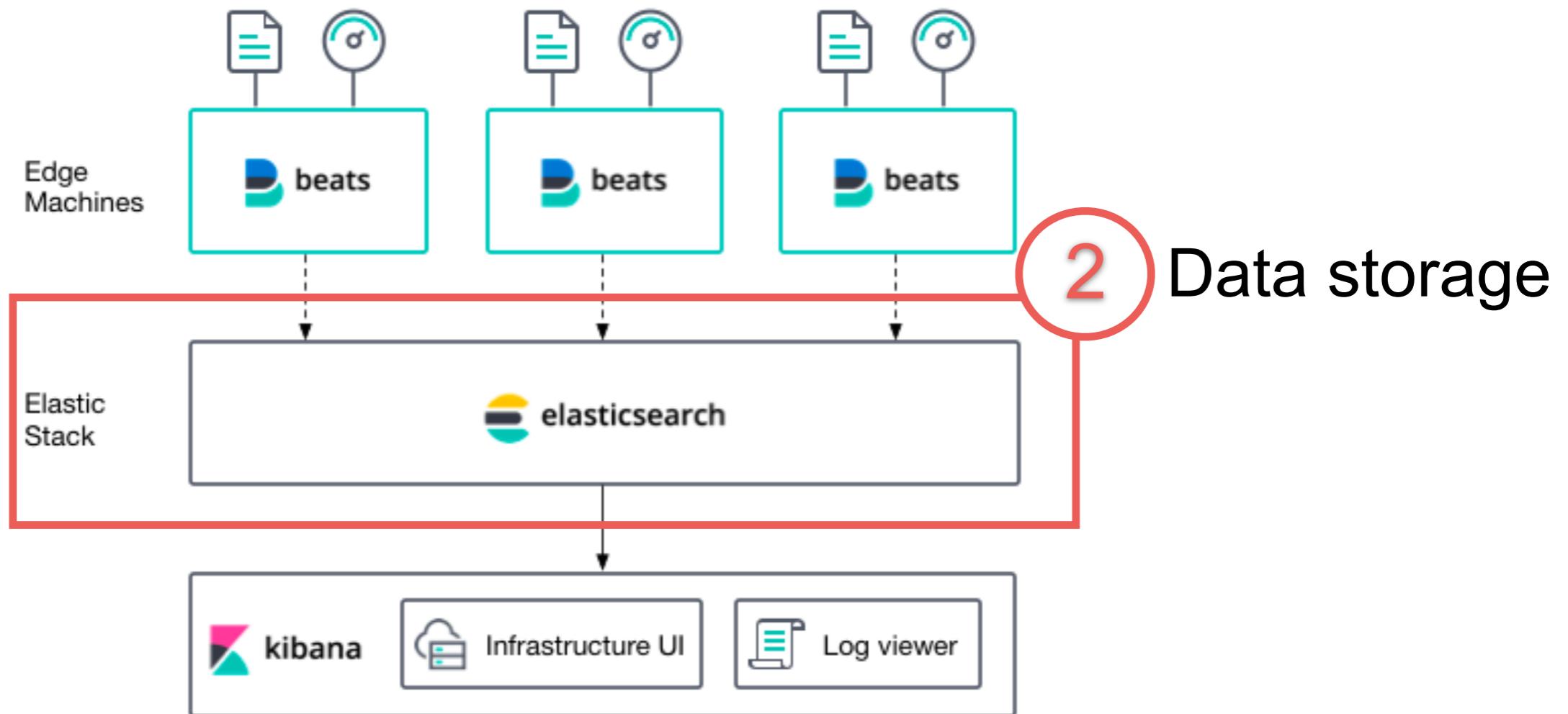
ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

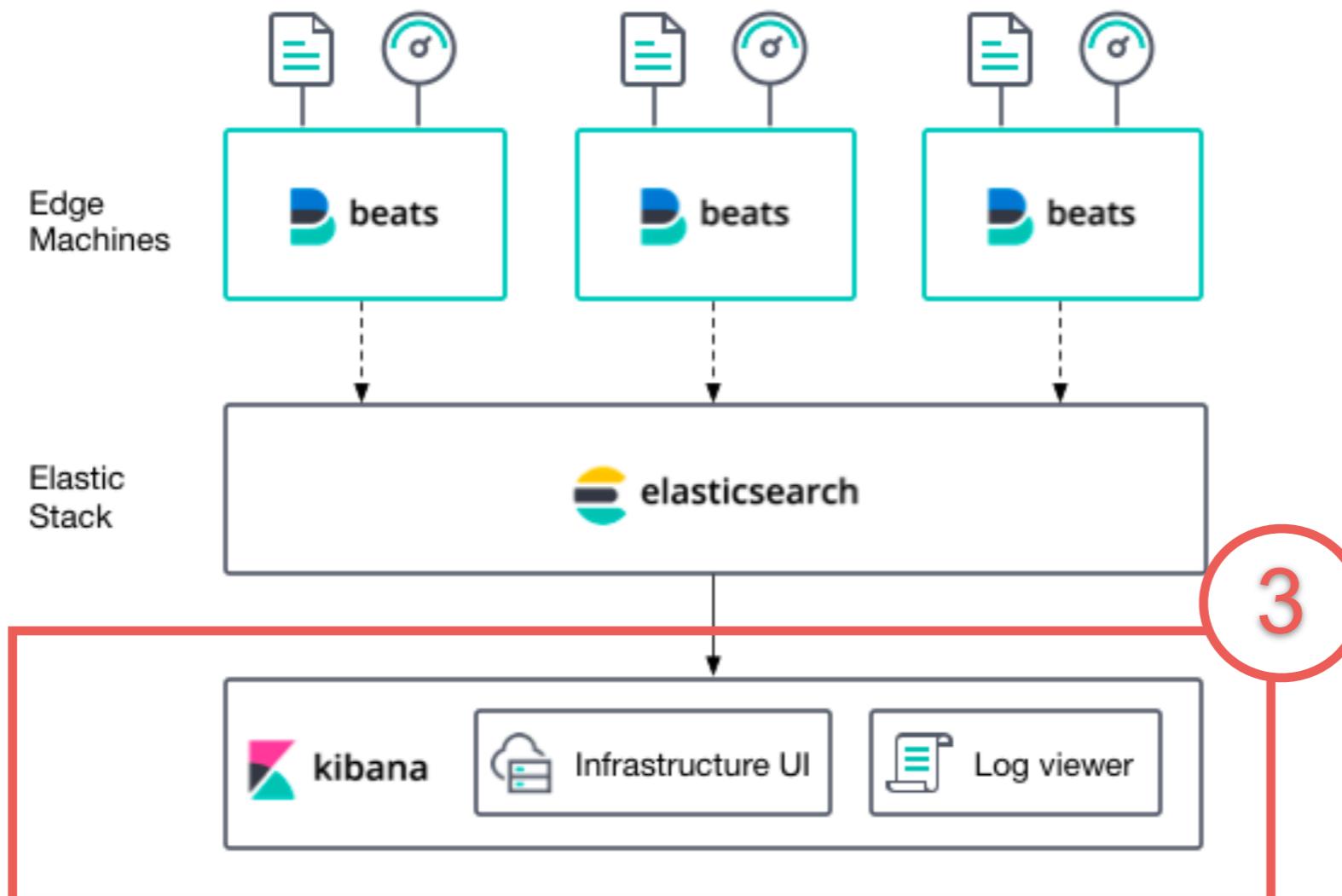
Infrastructure monitoring



Infrastructure monitoring



Infrastructure monitoring



Data
visualization



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Installation

Data Shippers



Metricbeat



Filebeat



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Add metrics to Kibana

Add Data to Kibana

All Logging Metrics Security analytics Sample data

Aerospike metrics

Fetch internal metrics from the Aerospike server.

Apache metrics

Fetch internal metrics from the Apache 2 HTTP server.

Ceph metrics

Fetch internal metrics from the Ceph server.

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 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.

Kafka metrics

Fetch internal metrics from the Kafka server.

Kibana metrics

Fetch internal metrics from Kibana.

Kubernetes metrics

Fetch metrics from your Kubernetes installation.

Logstash metrics

Fetch internal metrics from a Logstash server.

Memcached metrics

Fetch internal metrics from the Memcached server.

MongoDB metrics

Fetch internal metrics from MongoDB.



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Setup Metricbeat

[Home](#) / [Add Data](#)

Elasticsearch metrics BETA

The `elasticsearch` Metricbeat module fetches internal metrics from Elasticsearch. [Learn more.](#)

[View exported fields](#)

[Self managed](#)

[Elastic Cloud](#)

Getting Started

[macOS](#) [DEB](#) [RPM](#) [Windows](#)

1 Download and install Metricbeat

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

[Copy snippet](#)

```
curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.5.4-darwin-x86_64.tar.gz  
tar xzvf metricbeat-6.5.4-darwin-x86_64.tar.gz  
cd metricbeat-6.5.4-darwin-x86_64/
```



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Setup Metricbeat

Install Metricbeat

Config Metricbeat

Enable Elasticsearch module in Metricbeat

Start Metricbeat



Dashboard in Kibana

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

X Include system indices

Step 1 of 2: Define index pattern

Index pattern

index-name-*

You can use a * as a wildcard in your index pattern.

You can't use spaces or the characters \, /, ?, ", <, >, |.

> Next step

Your index pattern can match any of your **5 indices**, below.

kibana_sample_data_logs

metricbeat-6.5.4-2019.01.10

mobile

store

xxx

Rows per page: 10 ▾



ELK Stack

© 2017 - 2018 Siam Chamnkit Company Limited. All rights reserved.

Dashboard in Kibana

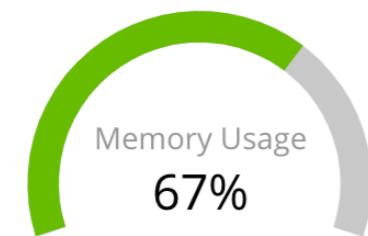
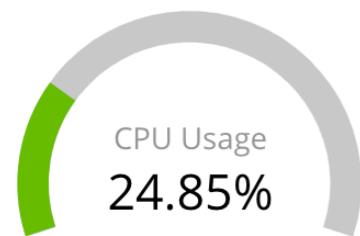
Dashboards

[Create new dashboard](#)

<input type="checkbox"/>	Title	Description	Actions
<input type="checkbox"/>	[Metricbeat Docker] Overview	Overview of docker containers	Edit
<input type="checkbox"/>	[Metricbeat Apache] Overview	Overview of Apache server status	Edit
<input type="checkbox"/>	[Metricbeat System] Containers overview	Overview of container metrics	Edit
<input type="checkbox"/>	[Metricbeat Golang] Overview	Overview of Go profiling information	Edit
<input type="checkbox"/>	[Metricbeat HAProxy] HTTP backend	HAProxy HTTP backend metrics	Edit
<input type="checkbox"/>	[Metricbeat HAProxy] Backend	HAProxy backend metrics	Edit
<input type="checkbox"/>	[Metricbeat HAProxy] Frontend	HAProxy frontend metrics	Edit
<input type="checkbox"/>	[Metricbeat System] Host overview	Overviw of host metrics	Edit



Host overview dashboard



Inbound Traffic
132.531KB/s
Total Transferred 45.333MB

Outbound Traffic
1.331MB/s
Total Transferred 638.012MB

In Packetloss
0
Out Packetloss 205

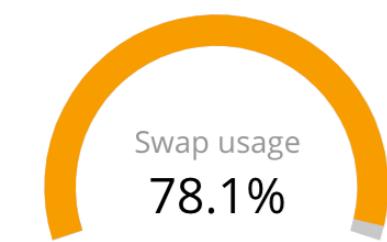
Swap usage [Metricbeat...]

Memory usage vs total

Number of processes [...]

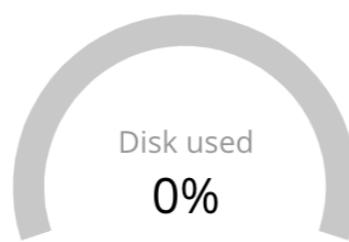
Disk used [Metricbeat S...]

Disk Usage [Metricbeat System]

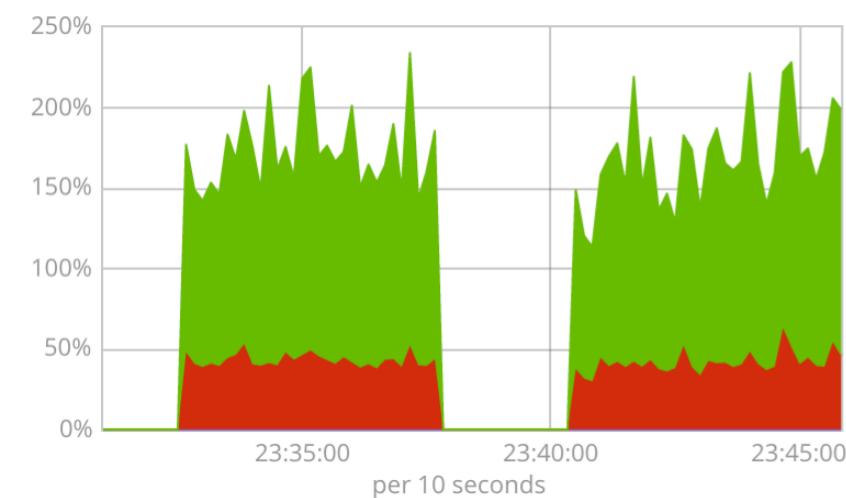


Memory usage
10.72GB
Total Memory 16GB

27
Processes

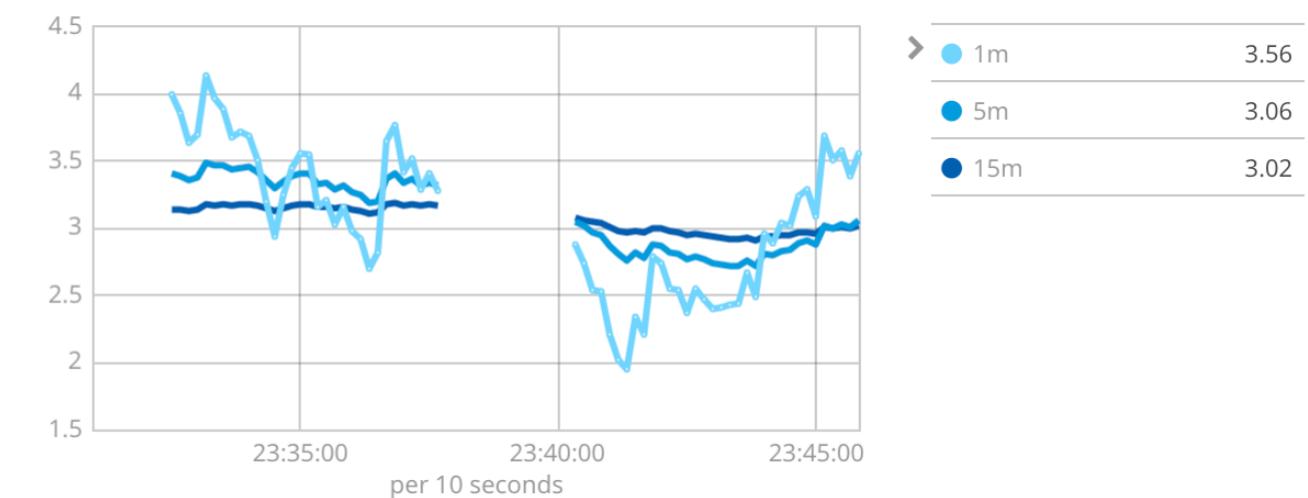


CPU Usage [Metricbeat System]



user	153.1%
system	45.7%
nice	0%
irq	0%
softirq	0%
iowait	0%

System Load [Metricbeat System]



ELK Stack

30

Try to setup Logging !!



Add logging to Kibana

Home

Add Data to Kibana

All

Logging

Metrics

Security analytics

Sample data



Apache logs

Collect and parse access and error logs created by the Apache HTTP server.



Elasticsearch logs

Collect and parse logs created by Elasticsearch.

IIS logs

Collect and parse access and error logs created by the IIS HTTP server.



Kafka logs

Collect and parse logs created by Kafka.



Logstash logs

Collect and parse debug and slow logs created by Logstash itself.



MySQL logs

Collect and parse error and slow logs created by MySQL.



Nginx logs

Collect and parse access and error logs created by the Nginx HTTP server.



PostgreSQL logs

Collect and parse error and slow logs created by PostgreSQL.



Redis logs

Collect and parse error and slow logs created by Redis.

System logs

Collect and parse logs written by the local Syslog server.

Traefik logs

Collect and parse access logs created by the Traefik Proxy.



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Monitoring with Kibana



Enable monitoring in Kibana

The screenshot shows the Kibana interface with a sidebar on the left containing various navigation items: Discover, Visualize, Dashboard, Timelion, Canvas, Machine Learning, Infrastructure, Logs, APM, Dev Tools, Monitoring, and Management. The 'Monitoring' item is highlighted with a red box and a large red circle with the number '1' over it. The main content area is titled 'Clusters' and displays a message: 'Monitoring is currently off'. It includes a heart icon with a pulse line, a brief description, and a note about cluster default settings. A blue button labeled 'Turn on monitoring' is present, also enclosed in a red box and circled with '2'.

Clusters

Monitoring is currently off

We checked the cluster defaults settings and found that `xpack.monitoring.collection.enabled` is set to `false`.

Would you like to turn it on?

Turn on monitoring



Monitoring in Kibana

The screenshot shows the Kibana interface with two main monitoring dashboards:

- Elasticsearch Dashboard:** Shows the status of the Elasticsearch cluster. It includes an Overview section with Version 6.5.4 and Uptime 10 hours, and a Nodes: 1 section showing Disk Available (61.76%) and JVM Heap (35.85%). The cluster health is yellow.
- Kibana Dashboard:** Shows the status of the Kibana instance. It includes an Overview section with Requests (4) and Max. Response Time (27 ms), and an Instances: 1 section showing Connections (0) and Memory Usage (16.17%). The Kibana health is green.

The left sidebar contains navigation links for Discover, Visualize, Dashboard, Timelion, Canvas, Machine Learning, Infrastructure, Logs, APM, Dev Tools, Monitoring (which is selected), and Management. At the bottom of the sidebar are buttons for Default and Collapse.



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Subscription of Kibana

	FREE OPEN SOURCE	BASIC	GOLD	PLATINUM
Kibana				
▼ Explore & Visualize	✓	✓	✓	✓
▼ Stack Management & Tooling	✓	✓	✓	✓
^ Stack Monitoring		✓	✓	✓
Full stack monitoring		✓	✓	✓
Multi-stack monitoring support			✓	✓
Configurable retention policy			✓	✓
Automatic alerts on stack issues			✓	✓
▼ Share & Collaborate	✓	✓	✓	✓
▼ Security			✓	✓
▼ Alerting			✓	✓
▼ Machine Learning		✓	✓	✓

<https://www.elastic.co/subscriptions>



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Subscription of Beat

	FREE OPEN SOURCE	BASIC	GOLD	PLATINUM
	Download		Request Info	Request Info
Beats				
✓ Data Collection	✓	✓	✓	✓
✓ Data Shipping	✓	✓	✓	✓
✓ Modules	✓	✓	✓	✓
^ Monitoring and Management		✓	✓	✓
Beats monitoring		✓	✓	✓
Centralized Beats management			✓	✓

<https://www.elastic.co/subscriptions>



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Collect data from ?

Elasticsearch nodes

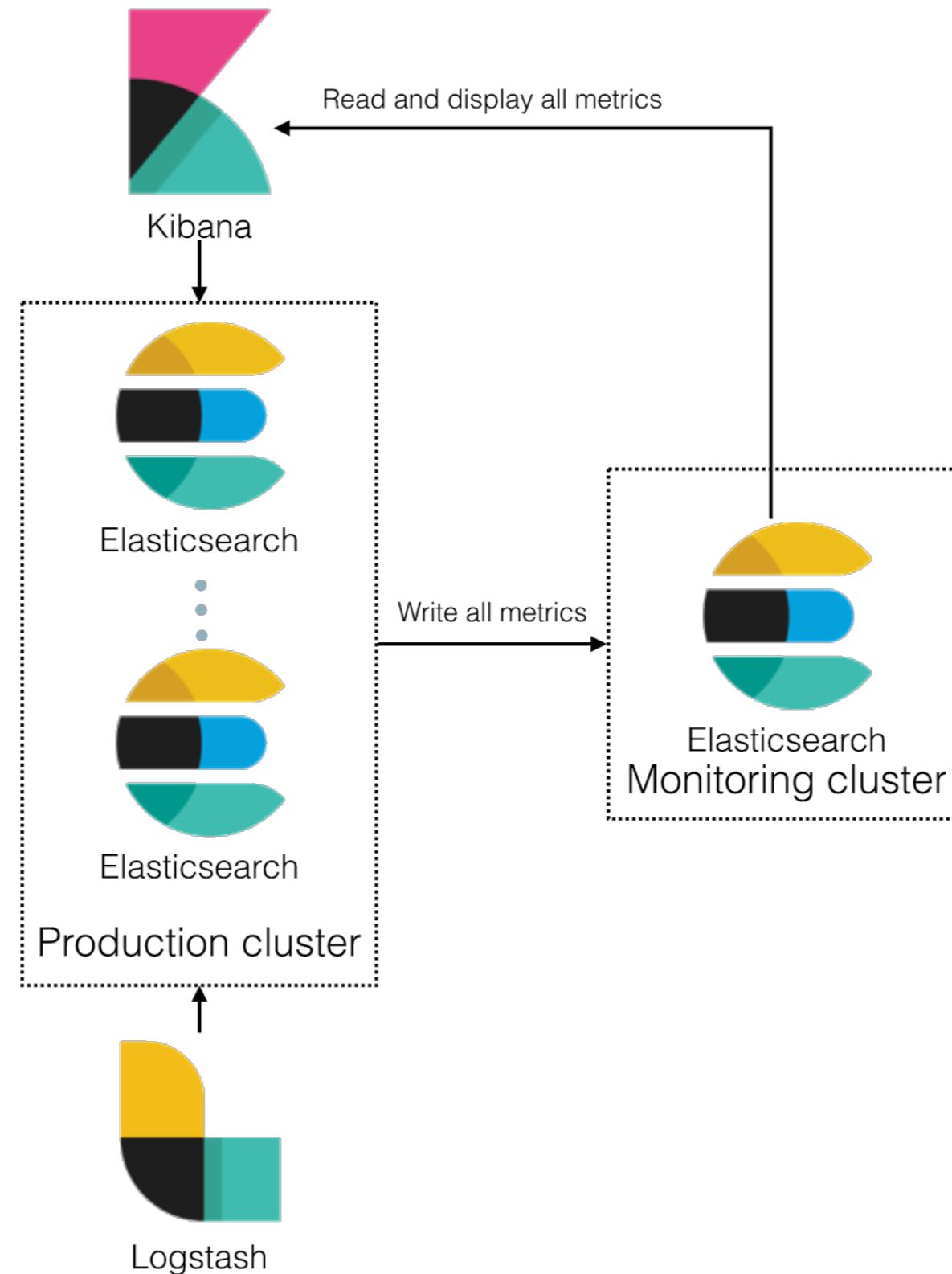
Logstash nodes

Kibana instances

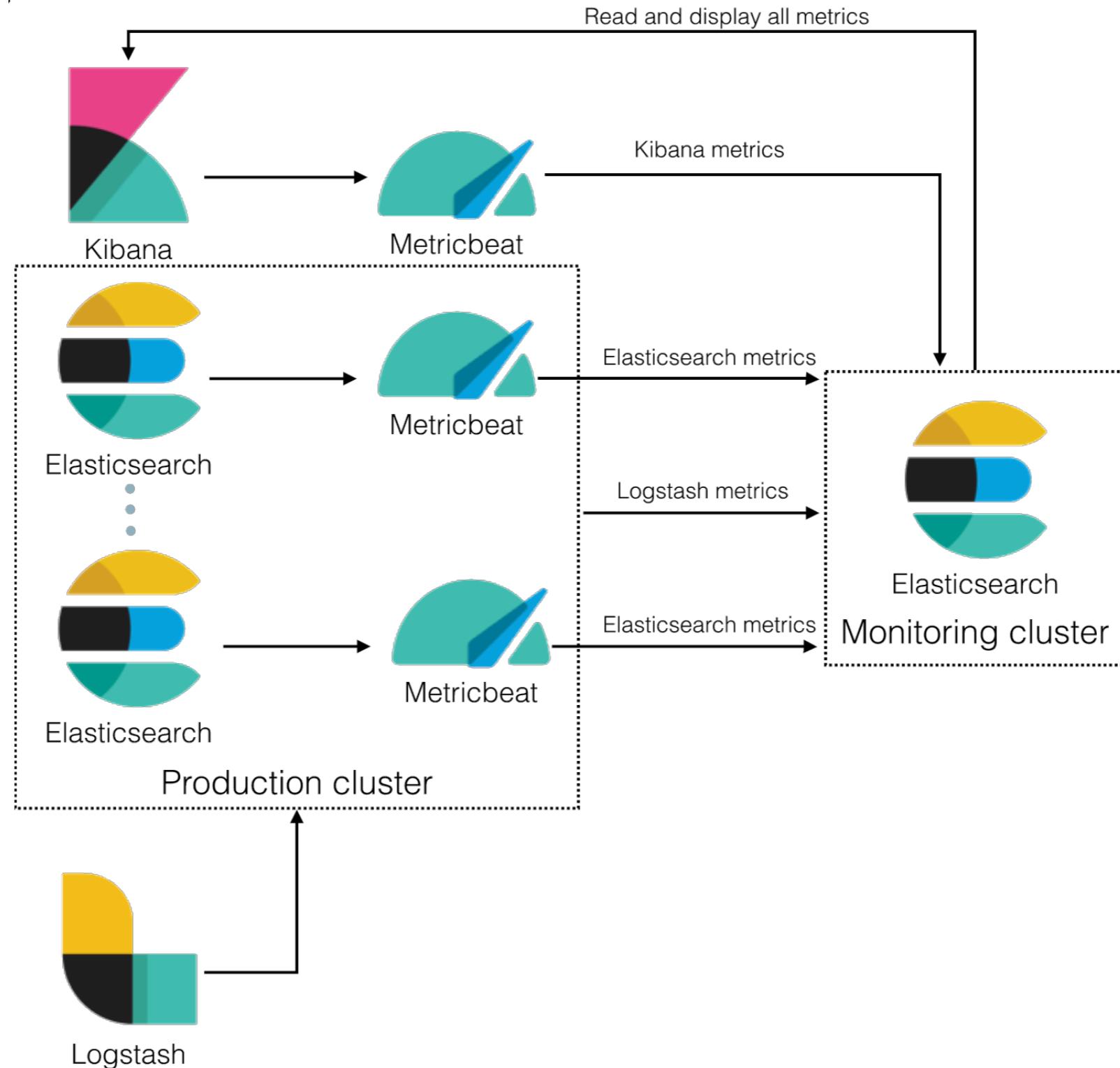
<https://www.elastic.co/guide/en/elasticsearch-stack-overview/6.5/xpack-monitoring.html>



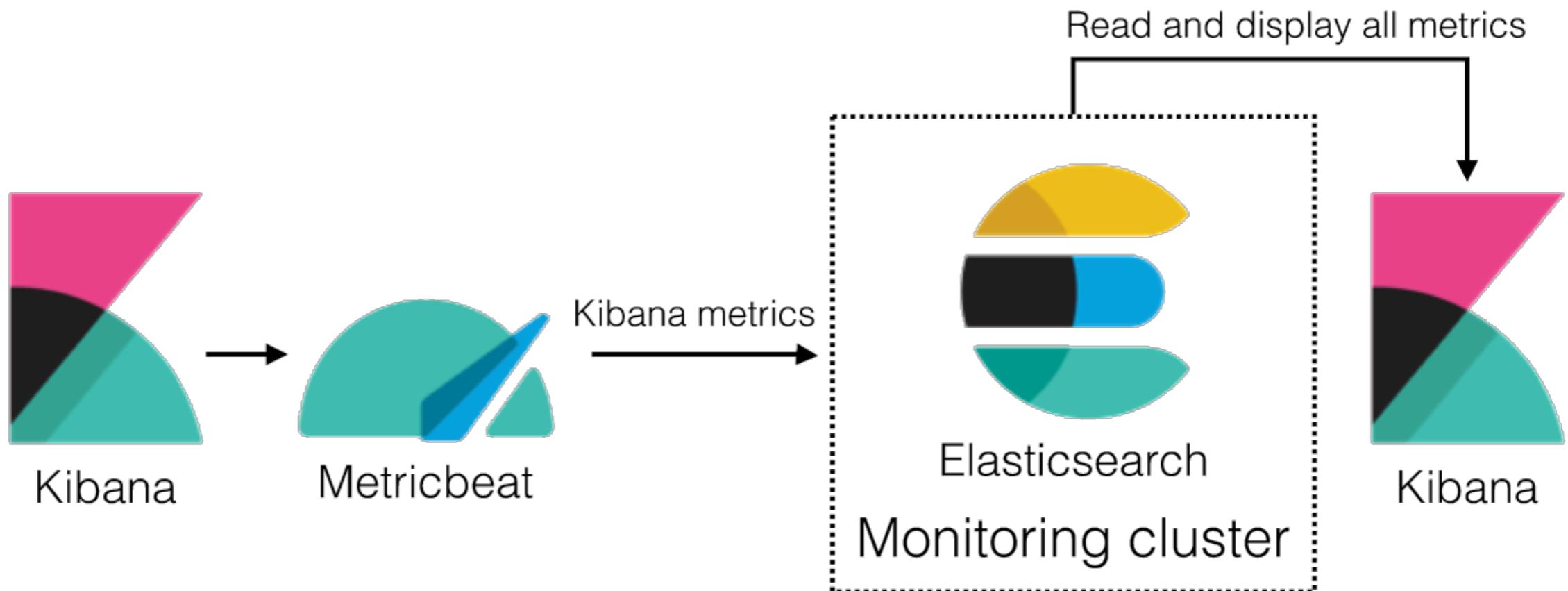
Recommend architecture



Elasticsearch 6.4 + (beta)



Try to separate kibana



Working with Logstash

<https://www.elastic.co/guide/en/logstash/current/index.html>



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

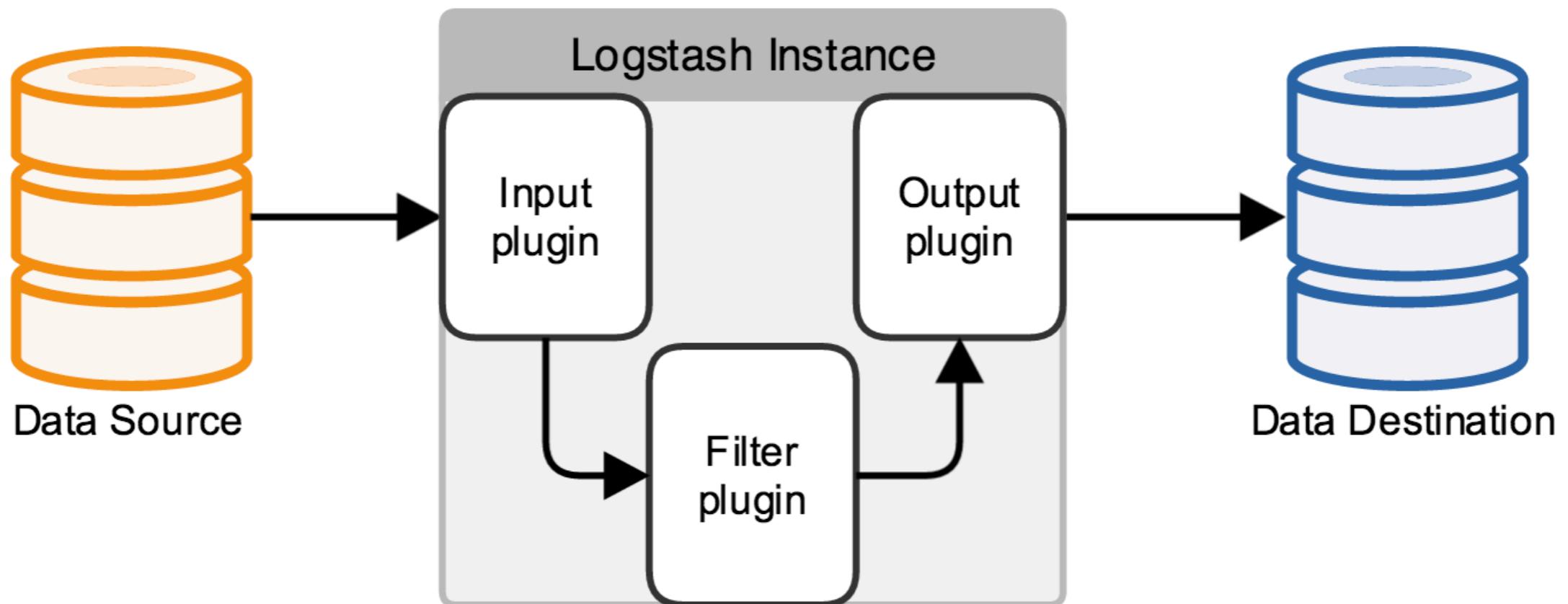
Logstash



Input
Filter
Output



Logstash



Inputs

File system

Syslog

Redis

Elasticsearch

Beats

More ...

<https://www.elastic.co/guide/en/logstash/current/input-plugins.html>



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Filters

Grok
Mutate
Drop
Clone
GeoIP
More ...

<https://www.elastic.co/guide/en/logstash/current/filter-plugins.html>



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Outputs

Elasticsearch
File system
StatsD
Graphite
More ...

<https://www.elastic.co/guide/en/logstash/current/output-plugins.html>



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Codecs

JSON
Multiple
Plain
RubyDebug
More ...

<https://www.elastic.co/guide/en/logstash/current/codec-plugins.html>



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Running Logstash

```
./bin/logstash -f your-config.yml
```

*Demo of configuration file
/workshop/grok*

<https://www.elastic.co/guide/en/logstash/current/running-logstash-command-line.html>



ELK Stack

© 2017 - 2018 Siam Chamnkit Company Limited. All rights reserved.

Design your input first !!



Use beats is better

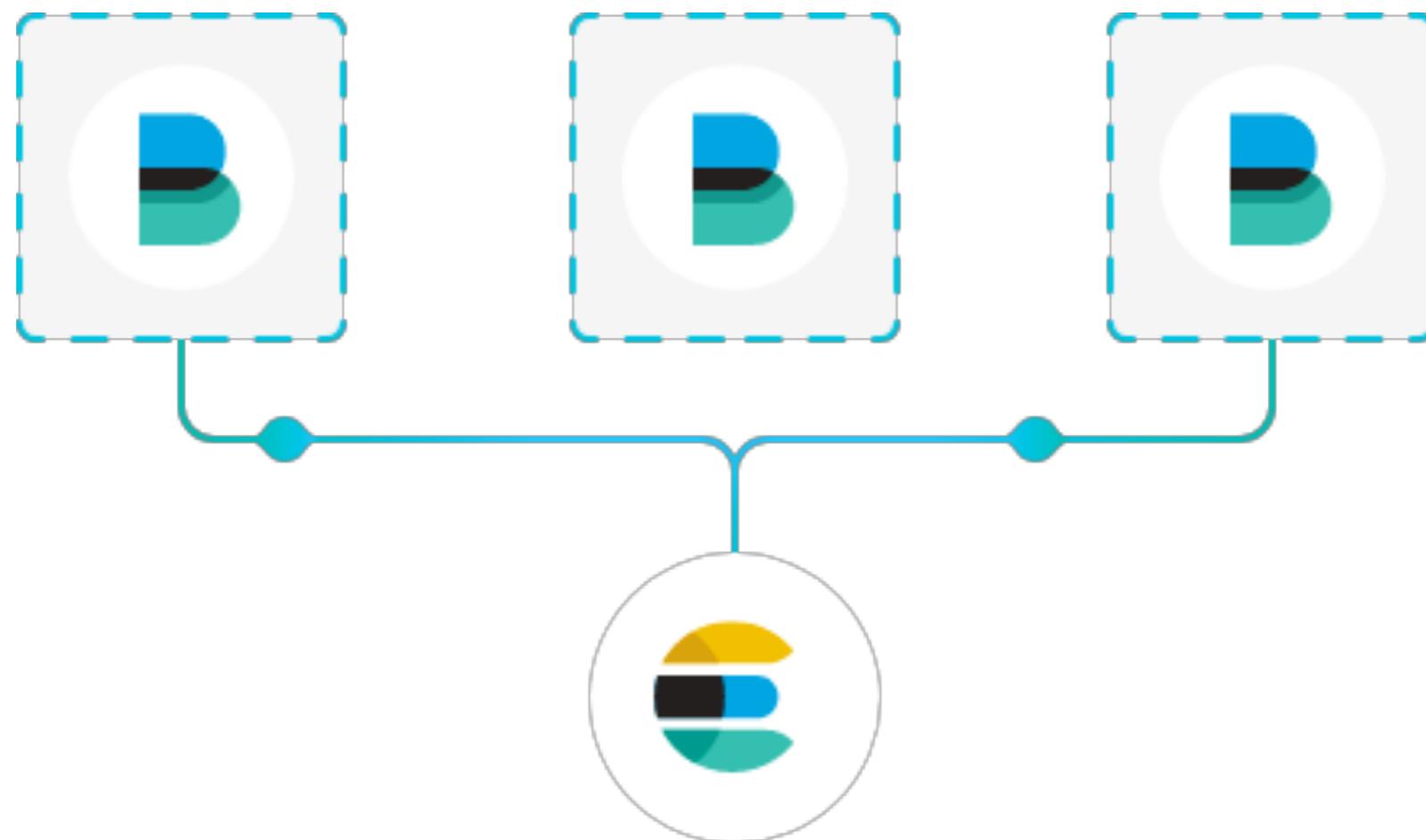
<https://www.elastic.co/products/beats>



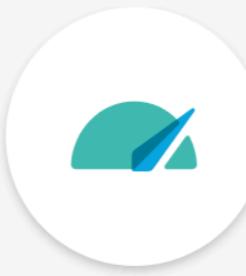
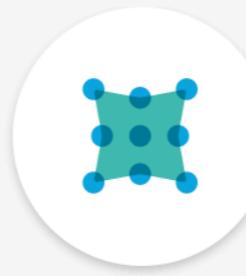
ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Beat



Beat

					
Filebeat Log Files	Metricbeat Metrics	Packetbeat Network Data	Winlogbeat Windows Event Logs	Auditbeat Audit Data	Heartbeat Uptime Monitoring



ELK Stack

© 2017 - 2018 Siam Chamnkit Company Limited. All rights reserved.

Example

```
$filebeat -e -c beat.yml -d "publish"
```

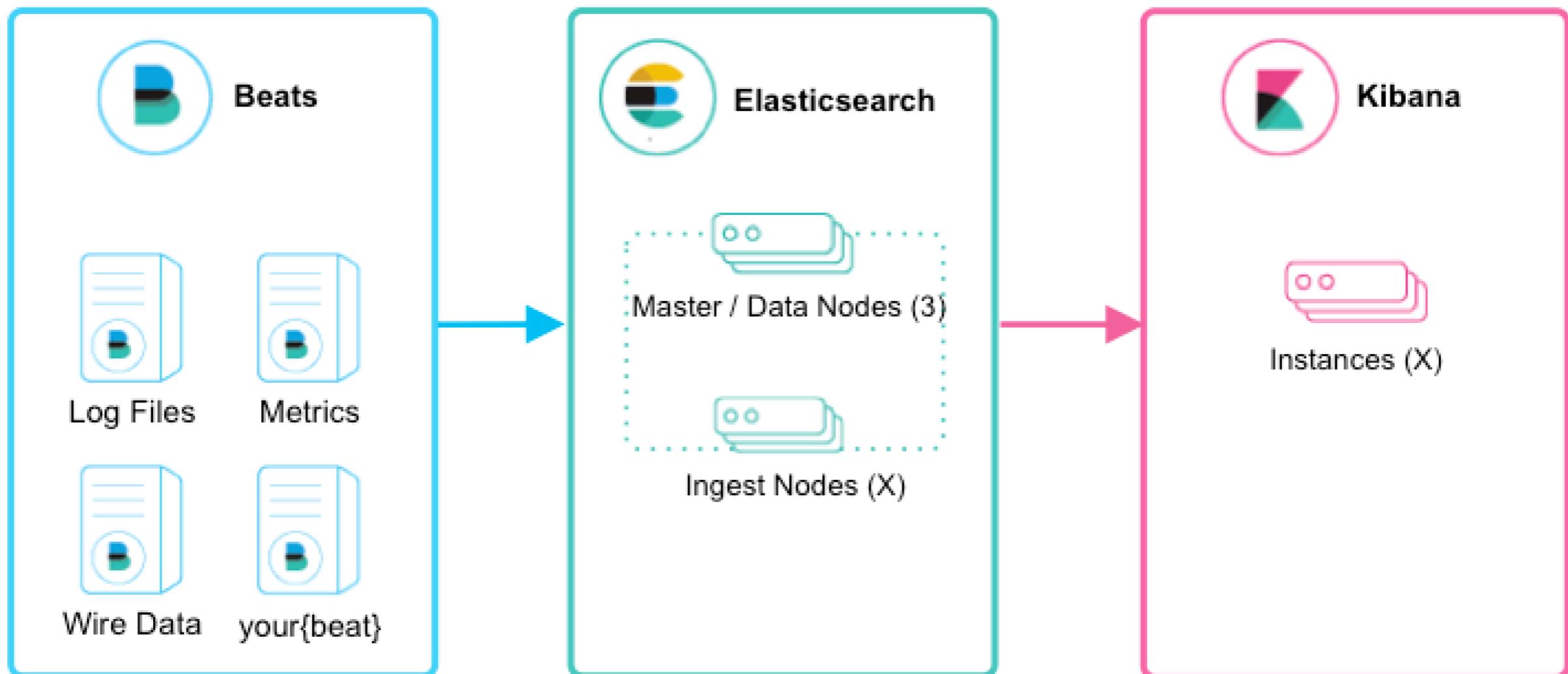
<https://www.elastic.co/guide/en/beats/filebeat/current/index.html>



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Beat and Logstash



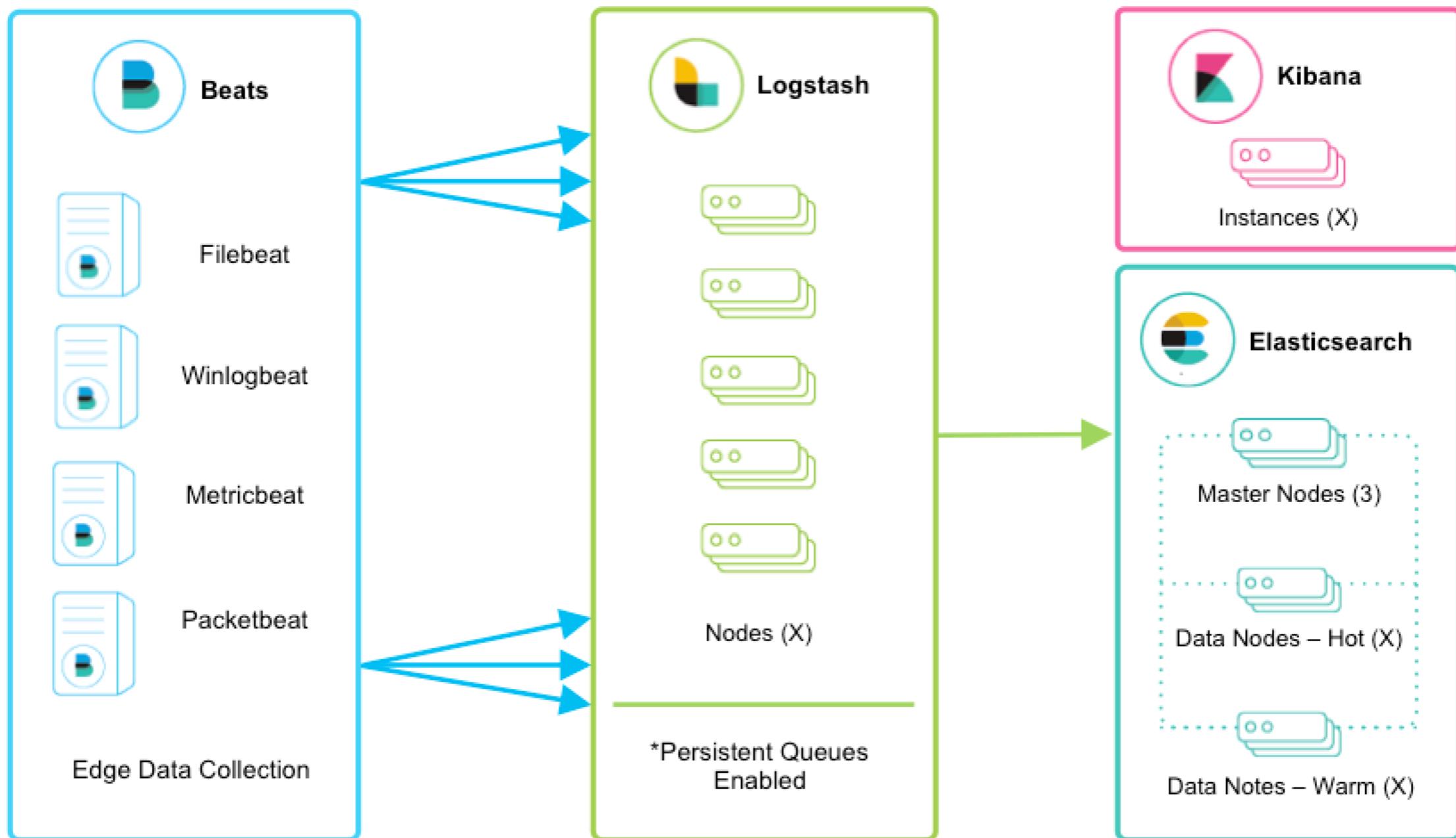
<https://www.elastic.co/guide/en/logstash/current/deploying-and-scaling.html>



ELK Stack

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Scaling



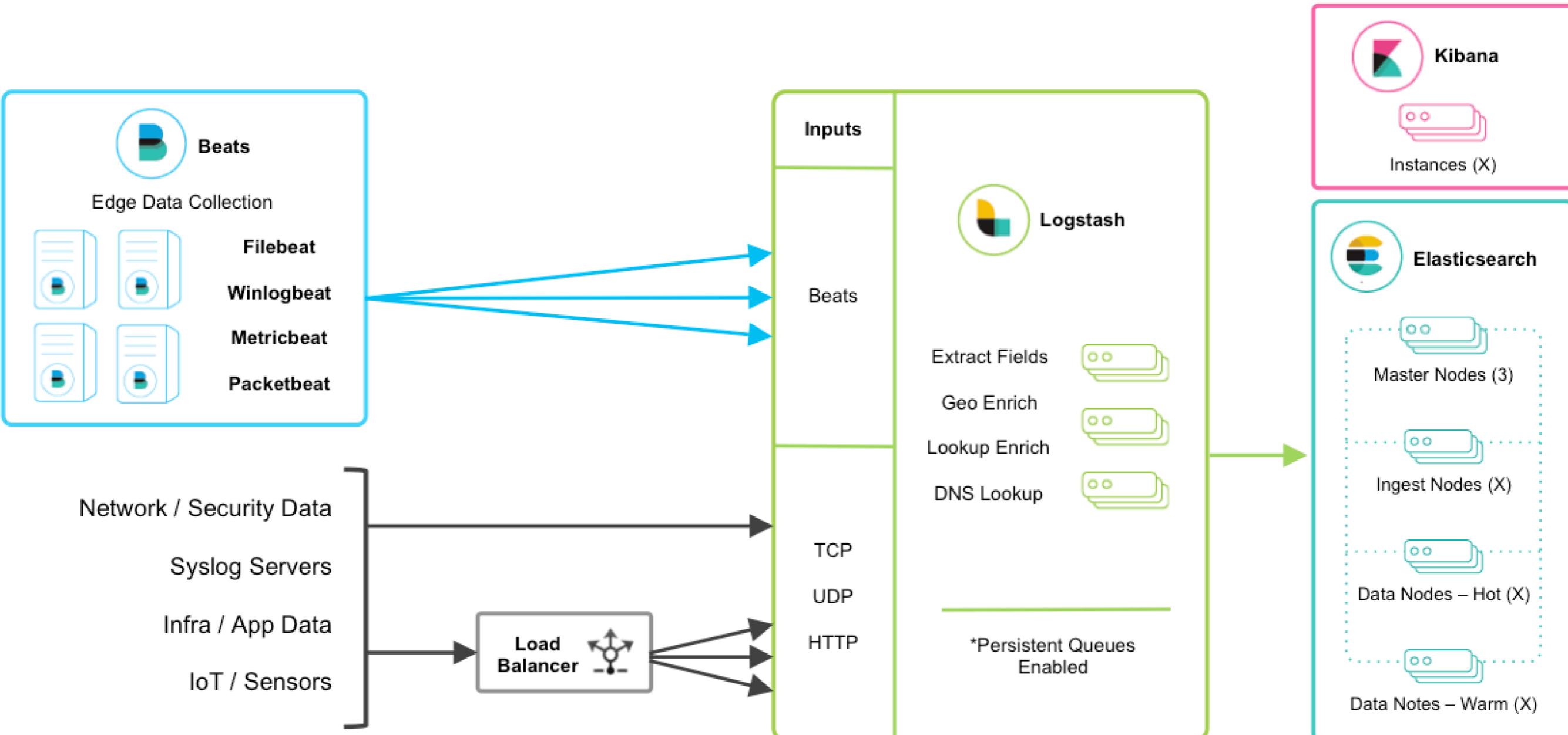
<https://www.elastic.co/guide/en/logstash/current/deploying-and-scaling.html>



ELK Stack

© 2017 - 2018 Siam Chamnkit Company Limited. All rights reserved.

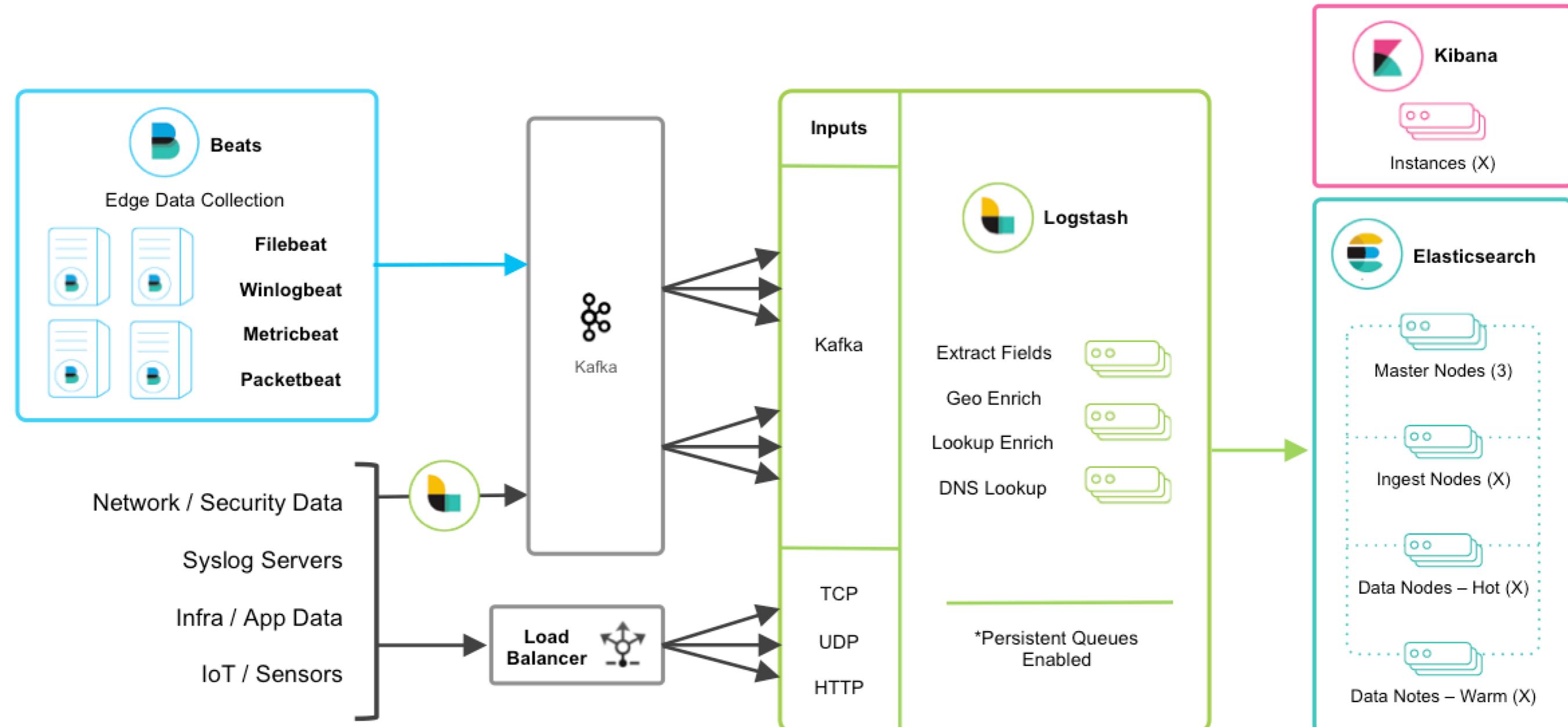
More data sources



<https://www.elastic.co/guide/en/logstash/current/deploying-and-scaling.html>



Use messaging Queue



<https://www.elastic.co/blog/logstash-persistent-queue>

